Logiciel SMS

Manuel d’utilisateur

SYSTEME DE GESTION DE SECURITE

9600-0429

© Group 4 Technology 2006

Tous droits de reproduction réservés. Toute reproduction d'un extrait quelconque de la présente publication, par quelque procédé que ce soit est interdite sans l'accord écrit préalable de Group 4 Technology.

Challenge House
International Drive
Tewkesbury
Glos
GL20 8UQ
UK

Telephone: +44 (0) 1684 850977

Système de gestion de sécurité Manuel d'utilisateur

Edition 6.0 – 25 janvier 2006

N° d'inventaire: 9600-0429

Microsoft et Windows sont des marques de commerce enregistrées de la Microsoft Corporation.
BACnet est une marque de commerce enregistrée d'ASHRAE.
Crystal Reports est une marque de commerce enregistrée de la sté Crystal Decisions.
Le logiciel de compression d'image se base en partie sur le travail de l'Independent JPEG Group.
Philips et MIFARE sont des marques de commerce enregistrées de Philips Electronics N.V.
HID est une marque de commerce enregistrée de HID Corporation.
i*CLASS* est une marque de commerce enregistrée de HID Corporation.
Texas Instruments est une marque de fabrique enregistrée de Texas Instruments Incorporated.
ENVS est une marque de commerce enregistrée de Group4 Technology Ltd.
GCS, GCS TopGuard et ProxiPen sont des marques de commerce enregistrées de GCS.
Tous les autres signes distinctifs sont des marques de fabrique de leurs propriétaires respectifs.

ENVS™

Composants vidéos MPEG-4 basés sur technologie ateme

Table des matières

Préface ..... **iv**

Chapitre 1: L'introduction dans la gestion de sécurité **1-1**

Au sujet du système de gestion de sécurité **1-1**
Le but 1-1

Les portes **1-1**
Comment avoir accès 1-1
Les alarmes et événements 1-2
La configuration du système 1-2
Les rapports/listes 1-3
Le système de partition (multi-sociétés) 1-3
Les fonctions standard 1-3
Les fonctions optionnelles 1-3

Les composants d'un système de gestion de sécurité **1-5**
Les lecteurs de cartes 1-5
Les boutons d'ouverture de porte 1-6
Le verrou de porte 1-6
La surveillance des portes 1-6
Le serveur et les PC-clients 1-6
L'imprimante 1-7
Les centrales de contrôle (nœuds) 1-7
Les modems 1-7
Les points de surveillance 1-7
Les sorties auxiliaires 1-8
Systèmes de vidéo-surveillance (CCTV) et de vidéo numérique 1-8
Panneaux d'intrusion/d'alarme 1-8
Système d'interphone 1-8

Les types de produit **1-9**
Les systèmes Lite Edition 1-9
Les systèmes Professional Edition 1-9
Les systèmes Enterprise Edition 1-9
Les systèmes Global Edition 1-9

Chapitre 2: Comment bien démarrer **2-1**

Ouvrir le logiciel de gestion de sécurité (SMS) **2-1**

Au sujet de l'interface utilisateur **2-2**
Les fenêtres de sélection et de définition 2-3

Au sujet de vos droits d'utilisateur **2-3**

Qu'est-ce qu'il faut faire ensuite? **2-4**

Chapitre 3: La gestion des cartes **3-1**

Au sujet de la fenêtre des détenteurs de cartes **3-1**
Créer ou trouver un détenteur de carte 3-1
Le nom de famille, le prénom et l'initiale 3-3
Le numéro de carte 3-3

Créer les détails de cartes **3-4**
La photo du détenteur de carte 3-4
Les dates actives et inactives 3-4
Le code PIN 3-5
Le code de bâtiment/client (Facility/Customer code) 3-5
La conception des badges et leur expiration 3-5
Les options de carte supplémentaires 3-5
L'état du détenteur de carte 3-5

Créer et accorder les droits d'accès **3-6**
Définir les codes de temps et les heures 3-8
Définir les jours fériés 3-10

Spécifier les coordonnées personnelles **3-11**

Localiser un détenteur de carte **3-13**

Chapitre 4: Produire les badges ID **4-1**

L'introduction **4-1**

Concevoir les badges **4-1**

Produire un badge de détenteur de carte **4-3**
Entrer les éléments de carte et prendre la photo du détenteur de carte 4-3
Approbation de la personne autorisée 4-3
Saisir la signature du détenteur de carte 4-3
Saisir l'empreinte digitale et les données biométriques de la main 4-4
Sélectionner et présenter la conception du badge 4-4
Imprimer le badge 4-5
Encoder le badge (la carte) 4-6

Chapitre 5: La gestion des visiteurs **5-1**

La création des visiteurs **5-1**

Les coordonnées des visiteurs **5-2**

Les coordonnées personnelles **5-2**

Les détails de carte de visiteur, les droits d'accès et la biométrie **5-2**

Les rapports de visiteurs **5-3**

Chapitre 6: La gestion de vidéo numérique **6-1**

Utiliser l'écran de matrice virtuel **6-3**

Utiliser l'écran de visionnage vidéo **6-4**

Utiliser la vérification vidéo **6-5**

Logiciel de sauvegarde sur serveur vidéo **6-6**

Utiliser l' unités du connecteur et camerás CCTV **6-7**
Visualiser une vue CCTV pendant l'acquittement d'alarme 6-7

Commandes vidéo numérique et commandes de commutateurs de vidéosurveillance **6-8**
Commandes des caméras de surveillance vidéo 6-8

Visionnage d'alarmes et de rapports **6-8**

Intégration graphique **6-9**

Chapitre 7: La surveillance des alarmes 7-1

Comprendre la surveillance des alarmes 7-1
Comment les nouvelles alarmes sont signalées 7-1

Les démarches à prévoir en cas d'une alarme 7-2
Regarder les détails d'une alarme 7-2
Installer les filtres d'alarme 7-3
Regarder une vue en graphique de l'endroit d'alarme 7-4
Acquitter une alarme 7-4
Réinitialiser l'alarme 7-6
Effacer l'alarme 7-6

Chapitre 8: Produire des rapports 8-1

L'introduction 8-1

Les rapports d'activité 8-1

Les rapports d'événements 8-2

Les rapports d'événements (Locator) 8-3

Rapports de cartes 8-3

Les rapports d'accès 8-4

Rapports visiteurs 8-5

Rapports de configuration 8-5

Les rapports de présence (roll call) 8-7
La configuration des rapports de présence 8-8
Surveiller le contrôle de présence 8-9

Chapitre 9: D'autres fonctions 9-1

Installer les profils d'utilisateurs et les comptes 9-1
Installer les profils 9-1
La création d'un compte d'utilisateur 9-2

Transmettre des commandes 9-3
Les commandes manuelles 9-3
Les commandes programmées 9-4
Les commandes de déclenchement 9-6

Regarder l'état des appareils 9-8

La gestion du niveau de risque 9-8

La gestion des rondes des gardiens 9-9

La gestion des graphiques 9-10

L'accès au Web 9-10

Les modes de lecteur 9-11
Le mode de carte et PIN 9-11
Le mode du code utilisateur 9-11
Le mode de commande de carte 9-12
Le mode de carte-clé 9-12
Le mode du code client seulement 9-12
Le mode du code client seulement – le mode de non-mémorisation 9-12
Le mode Activer/Désactiver 9-12

Le mode d'empreinte digitale 9-12
Le mode de contrainte (Duresss mode)....9-13
Le mode d'effacer suite à un PIN erroné 9-13
Le mode de bascule (Toggle mode)....9-13
Le mode à deux cartes....9-13
Le mode d'inhibition du lecteur....9-13
Les modes d'antipassback....9-13

La sauvegarde et l'archivage des données....9-13

Installations pour multi-sociétés....9-14
Les bénéfices d'un système unique....9-14
Groupes de sociétés – protéger les informations privées....9-14
Partager les appareils pour les droits d'accès....9-15
Le routage des alarmes....9-15

Préface

Le présent manuel d'utilisateur a pour objectif de vous instruire de la terminologie et des outils de la gestion de sécurité et de vous familiariser avec ces moyens. Ce manuel ne veut pas essayer de décrire les détails de chaque option dans toutes les fenêtres; le programme d'aide *Online Help* étant disponible à cette fin.

Le chapitre 1 constitue une introduction dans la gestion de sécurité et devrait être lu par tout un chacun qui ne se connaît pas dans la matière et qui a à gérer ou à mettre en œuvre le système. Tous les autres chapitres entrent plus dans les détails des caractéristiques principales.

Les documents suivants fourniront des informations supplémentaires, qui pourraient servir à installer des modules ou utilitaires optionnels, tels que:

- *Installation de contrôle du bâtiment et Manuel d'utilisateur*
- *Guide d'utilisation du lecteur d'empreinte digitale 813*
- *Répertoire Installation du Manager de synchronisation et Manuel d'utilisateur*
- *Installation du Manager des rondes des gardiens et Manuel d'utilisateur*
- *Installation d'interface d'intrusion et Manuel d'utilisateur*
- *Guide de configuration du module NIC*
- *Installation d'accès au Web et Manuel d'utilisateur*
- *Installation du kit de développeur XML et Manuel d'utilisateur*

Installation du Manager du niveau de risque et Manuel d'utilisateur

Chapitre 1: L’introduction dans la gestion de sécurité

Au sujet du système de gestion de sécurité

Le but

Le système de gestion de sécurité (Security Management System) est une puissante solution intégrée pour les organisations nécessitant des mesures de sécurité automatisées. Le système comprend des dispositifs matériels et logiciels, qui peuvent être modifiés de façon à répondre aux besoins particuliers des entreprises de toutes tailles.

En fonction des composants achetés le système offre des options de contrôle, de surveillance et d'enregistrement centralisé des différents aspects de la sécurité, ceux-ci incluant le contrôle d'accès, la télésurveillance, le stockage et le visionnage vidéo numérique, ainsi que la détection des infractions, l'organisation des tours de garde et la gestion de l'interphone.

Le logiciel de gestion de sécurité

Votre système de gestion de sécurité (SMS software) est pourvu d’un logiciel qui fonctionne avec l’aide du système d’exploitation intégré dans le PC sur la base de Microsoft® Windows®.

Le logiciel SMS inclut une large gamme de caractéristiques standard complétée par un grand choix de modules supplémentaires de logiciel entièrement intégré pour assurer un niveau plus élevé d’efficience, de flexibilité et d’efficacité.

Le logiciel vous permet de réaliser des tâches telles que l’installation des règles du contrôle d’accès, la conception et l’impression de badges, il gère les visiteurs, représente les alarmes, produit des rapports, contrôle les caméras CCTV, défile les enregistrements CCTV du serveurs vidéos numérique or du magnétoscopes et surveille le système. Des possibilités de surveillance des alarmes d’un usage facile sont offertes pour être mises en œuvre par les gardiens ou un autre personnel de sécurité.

Les portes

Dans le présent manuel d’utilisateur on parle en général du terme „porte”. Le système peut être prévu à contrôler toute sorte de portes, à commencer par la porte à tourniquet en passant par la porte pivotante jusqu’à la porte d’étage d’un ascenseur, tout en soulignant la flexibilité inhérente au produit respectif.

Comment avoir accès

Pour accéder à une zone d’accès contrôlée toute personne présente normalement une carte, connue aussi comme „badge”, au lecteur se trouvant à côté de la porte. L’entrée du code d’identification personnel (PIN) peut également être nécessaire ou l’empreinte digitale pour les lecteurs

biométriques. Le système décide alors si l'accès est permis ou non compte tenu des règles définies au préalable, appelées les droits d'accès. Si l'accès est permis, la porte se déverrouille automatiquement.

Les droits d'accès spécifient à quel moment lequel des lecteurs (respectivement portes) peut-être utilisé par la personne autorisée. On définit ces règles en mettant en œuvre le logiciel de gestion de sécurité sur un ordinateur. Les droits d'accès peuvent changer non seulement d'un jour à l'autre, mais aussi pendant des jours fériés spécifiés, de sorte qu'ils maintiennent la sécurité de votre bâtiment pendant les périodes de vacances, de fermeture ou d'autres jours fériés à déterminer.

Une carte de contrôle d'accès comprend un numéro unique qui permet l'identification du détenteur de carte par le système. Le numéro sur la carte peut avoir été ajouté par le fabricant du système ou le spécialiste l'ayant installé, ou vous disposez vous-même d'un encodeur.

Il y a plusieurs types de lecteurs différents. Dans certains cas il faut tirer une carte à travers une fente, dans d'autres cas il suffit de faire passer la carte tout près du lecteur.

Les alarmes et événements

Le système surveille en permanence toutes les activités qui se passent sur les appareils comme les lecteurs, portes et points de surveillance et il enregistre toutes les actions importantes ayant eu lieu. Il enregistre les situations, lorsque l'accès est assuré, lorsque les portes sont fermées, et même dans des conditions plus sérieuses, p.ex. lorsqu'une porte a été ouverte avec violence ou lorsqu'une carte perdue par le propriétaire a été introduite par un autre. Chacune de ces conditions est classée comme une alarme ou un événement selon l'importance, les alarmes ayant la priorité absolue.

Les éléments de toutes les alarmes peuvent être affichés sur un ordinateur pour l'attention immédiate d'un gardien et ils sont enregistrés pour des rapports futurs. Les événements sont simplement répertoriés aux fins d'établir des rapports. Les alarmes et événements peuvent tous être relus dans des rapports, ceux-ci pouvant être imprimés automatiquement à intervalles réguliers.

On peut également installer une caméra vidéo, une sirène ou tout autre appareil qui réagit automatiquement dès qu'un événement ou une alarme se produisent. La possibilité de connecter de cette manière le système à des sirènes ou d'autres soi-disant „sortie auxiliaires" se fait par des commandes de déclenchement (trigger commands) (connues comme commandes conditionnelles ou IF = SI, THEN = ALORS, WHEN = QUAND). Les commandes de déclenchement sont des caractéristiques très puissantes qui permettent une flexibilité extrêmement grande sans trop de complexité.

Grâce au module de gestion d'alarmes à distance, élément du logiciel de gestion de sécurité, on peut diriger les alarmes par courrier électronique à l'adresse du personnel d'entretien ou de sécurité.

La configuration du système

Votre système de gestion de sécurité possède une grande variation de modes d'opération configurables, ce qui vous met en état d'exploiter le système pour vos besoins spécifiques. Certains modes qui vous sont utiles sont repris pendant l'installation du système, certains d'autres peuvent être activés ou désactivés à volonté, peut-être en tant qu'un résultat de commandes de déclenchement. On peut p.ex. introduire les règles d'antipassback qui évitent que les gens ne remettent leurs cartes à aucune autre personne, ou il est possible d'intégrer un lecteur de cartes dans le mode dit de „card-and-PIN" (carte et code d'identification personnel) de sorte que l'entrée du code PIN en même temps que celle de la carte soient forcément nécessaires.

La possibilité d'adapter le système à l'utilisateur d'une manière à ce que seulement ces caractéristiques soient retenues qui servent aux exigences de votre utilisateur et qu'il puisse réduire l'entraînement de l'opérateur à un minimum. Le système permet à ces usagers qui ont d'autres besoins d'être présentés par différentes caractéristiques. La possibilité d'adapter le système à

l'utilisateur de plusieurs autres manières démontre à quel point sa conception dispose d'une flexibilité inhérente et de la capacité de répondre exactement à vos exigences sans compromettre pour autant la facilité d'usage.

Les rapports/listes

Le logiciel permet d'établir toute une gamme de rapports, ou sur une base dite ad hoc ou automatiquement à des heures et jours prédéterminés. Bon nombre de rapports peuvent être adaptés par l'utilisateur afin qu'il puisse obtenir exactement les informations demandées. Ils vous mettent en mesure d'avoir la plupart des informations mises à jour concernant l'état de votre système et peuvent fournir une liste d'événements dans laquelle figurent les violations de la sécurité tentées.

Le système de partition (multi-sociétés)

Un des atouts les plus forts de ce système de gestion de sécurité consiste dans la possibilité d'application au sein d'un immeuble où il y a plus d'une société, peut-être à longue durée de bail. Le système assure de tenir secret les détails privés des cartes de chaque société vis-à-vis des autres, un seul utilisateur ayant le droit exclusif de gérer l'ensemble du système.

Dans la plupart des cas nous partons pour ce manuel du fait que l'installation du système est utilisée par une entreprise unique. Nous expliquons les effets de la mise en œuvre du système dans un environnement à plus d'une seule entreprise à la page 9-14 dans le paragraphe intitulé:*Installations pour multi-sociétés.*

Les fonctions standard

Les fonctions standard du logiciel de gestion de sécurité incluent le suivant:

- une interface utilisateur conviviale et pouvant être mise à jour
- contrôle complet des droits d'accès (spécifier „qui" a le droit d'aller „où" et „quand")
- gestion facile de cartes, y compris modifications de blocs
- gestion d'alarmes dynamique
- interface graphique de plans (p.e. afficher alarme sur la graphique de plans de bâtiment).
- conception et impressions de badges
- partition de bases de données
- autorisations de log in contrôlant l'accès des utilisateurs aux fenêtres et options de menu affichées
- options de vastes rapports
- gestion des visiteurs
- gestion dite d'antipassback
- contrôle simple du matériel par des commandes manuelles et automatisées
- système général d'aide en ligne rapporté au contexte

Les fonctions optionnelles

Les fonctions optionnelles incluent le suivant:

- encodage de cartes à bande magnétique
- gestion du niveau de risque
- kit de développeur XML
- interface de contrôle du bâtiment (BACnet®)
- encodage de cartes à mémoire
- intégration de commutation CCTV et d'enregistreur vidéo numérique

- Edge-of-Network Video Servers (ENVS) pour enregistrer de vidéo numérique, sauvegarde et play-back
- intégration du contrôle Intercom
- importation et exportation des données de cartes
- rondes des gardiens et intégration avec GCS TopGuard®
- contrôle de sûreté de présence (mustering)
- intégration de tableaux d'alarme (interface d'intrusion)
- alarmes de dial in et dial-out (de connexion/de déconnexion)
- alarmes par courrier électronique
- accès via le Web

Les composants d’un système de gestion de sécurité

La figure 1.1 présente quelques-uns des composants principaux du système de gestion de sécurité. Ci-après sont décrits les buts de chaque composant.

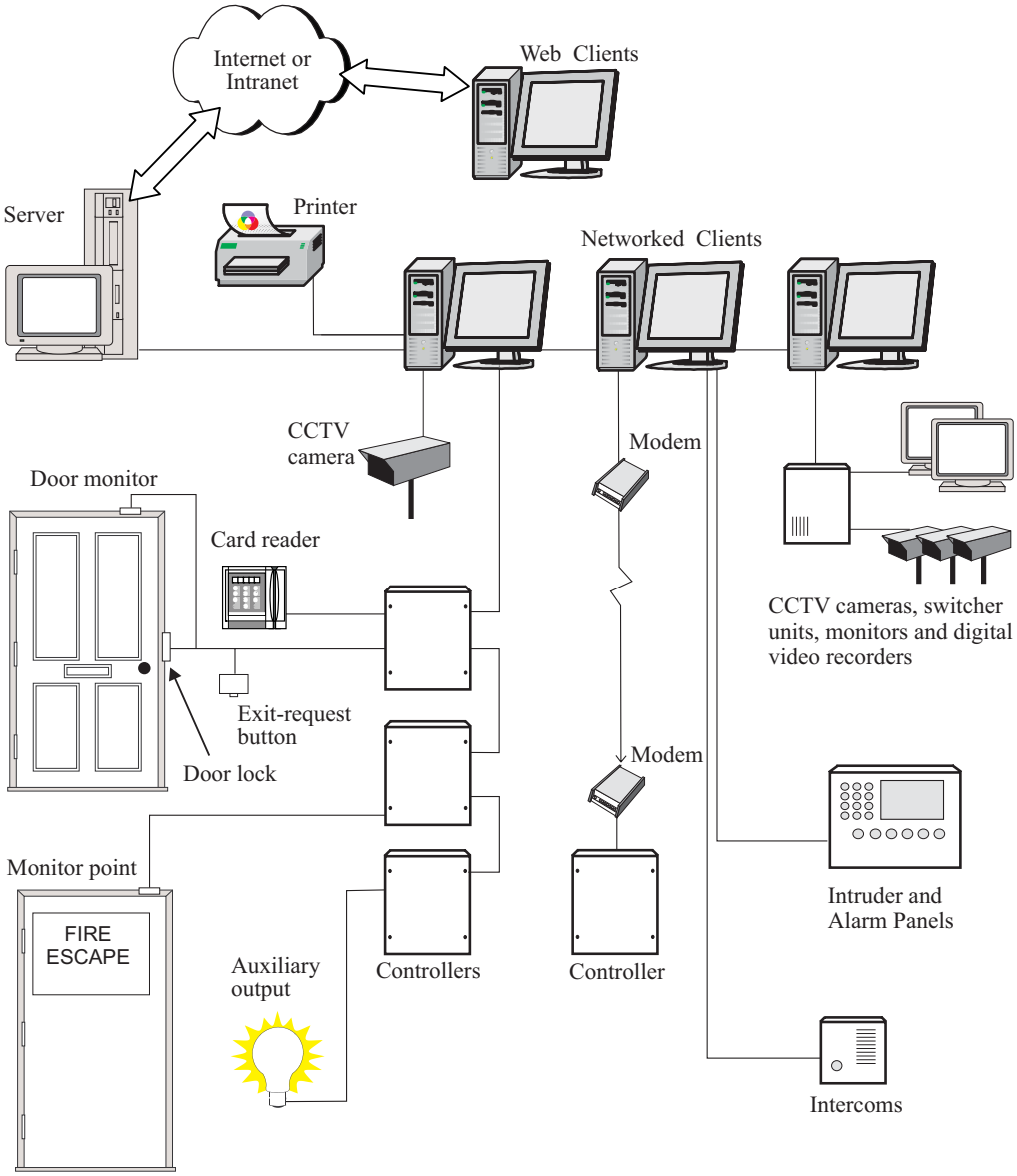


Figure 1.1: Les composants du contrôle d’accès

Les lecteurs de cartes

Les lecteurs de cartes permettent aux personnes de réaliser les transactions du contrôle d’accès. Le lecteur de cartes lit le numéro de carte de la personne respective et transmet cette information à la centrale (au nœud) qui décide si son accès est autorisé ou non, c’est-à-dire si la porte est à déverrouiller ou pas.

Chaque lecteur est affecté à une porte spécifique et se trouve, par conséquent, tout près de cette porte pour permettre de l'ouvrir, avant de la reverrouiller.

Les boutons d'ouverture de porte

Lorsqu'on appuie sur les boutons d'ouverture de porte, une porte se déverrouille. Normalement ils sont positionnés à côté d'une sortie pour permettre aux gens ayant libre accès de quitter de la même manière les locaux.

Le verrou de porte

Le verrou de porte s'ouvre après une transaction d'accès effectuée avec succès ou après l'appui sur un bouton d'ouverture de porte. La porte se referme automatiquement après un temps prédéterminé (normalement quelques secondes). La porte peut être déverrouillée en permanence et refermée suivant des commandes programmées (Cf. page **Error! Bookmark not defined.**), ce qui est très utile pendant les heures de pointe.

La surveillance des portes

Chaque porte est pourvue d'un contact de contrôle qui détecte les moments quand la porte est ouverte et quand elle est fermée. Cette information donne la possibilité à la centrale (au nœud) de constater p.ex. si la porte a été forcée ou tenue ouverte pour une durée trop longue.

Le serveur et les PC-clients

Le serveur, que l'on ne devrait jamais déconnecter, constitue le PC qui maintient et gère les bases de données du système de gestion de sécurité. Toutes les données concernant le système de gestion de sécurité, y compris les détenteurs de cartes, les droits d'accès et les alarmes, sont mémorisées dans les banques de données du serveur. Le serveur assume donc aussi différentes fonctions comme le traitement des transactions faites aux lecteurs de contrôle d'accès, le lancement des commandes de déclenchement ou programmées via les contrôleurs et l'introduction de rapports prévus.

D'autres ordinateurs, lesdits „clients", peuvent être connectés au serveur par l'intermédiaire d'un réseau. Les „clients" fournissent l'interface utilisateur pour le logiciel de gestion de sécurité. Ils permettent de réaliser des tâches telles que la configuration de détenteurs de cartes, la spécification des droits d'accès, l'impression de badges, la surveillance des alarmes, l'établissement de rapports et contrôler, enregistrer ou visionner vidéos d'un magnétoscope numérique (CCTV). Ils fournissent également les ports de communications pour la gestion du matériel de sécurité installé tout autour du bâtiment, p.ex. les nœuds qui commandent les portes et les lecteurs.

Plusieurs clients peuvent être mis en œuvre en même temps jusqu'à une limite qui est déterminée par le système fourni. Le nombre des clients requis dépend dans la plupart des cas du nombre des nœuds et du matériel de gestion de sécurité utilisés tout comme du nombre des usagers qui ont besoin de l'emploi du logiciel de gestion de sécurité. Dans un système de taille importante il se peut que les clients nécessaires sont nombreux et qu'ils sont prévus chacun à des buts différents. Chaque utilisateur du logiciel de gestion de sécurité est privilégié de certains droits de login, ce qui se répercute sur la gamme des fenêtres pouvant être ouvertes et sur les fonctions à assumer.

Les alarmes peuvent être transmises à chacun des clients en fonction de l'heure du jour ou du jour de la semaine, voire même des jours fériés. Ceci inclut la possibilité d'afficher p.ex. les alarmes sur le PC du réceptionniste pendant la journée ou du gardien pendant la nuit.

Certains clients peuvent être désignés à un but spécial. Les „clients Web" disponibles par le module d'accès optionnel Web (Web Access Module) permettent la connexion à distance via Internet ou Intranet.

L’imprimante

Une imprimante permet d’imprimer les rapports ou le contenu de la fenêtre à un moment donné. Toutes les imprimantes compatibles avec Windows s’approprient à cette fin. Des imprimantes spéciales sont offertes pour les badges et l’encodage optionnel des cartes.

Les centrales de contrôle (nœuds)

Les centrales de contrôle, soit les nœuds, sont le „cerveau“ du système de gestion de sécurité. En utilisant une copie des règles importantes qui ont été installées sur le PC-client, les nœuds commandent tous les appareils, y compris les lecteurs, les portes, les points de surveillance et les sorties auxiliaires. Un nœud peut décider indépendamment, si un accès est autorisé ou non, et réagir d’une manière voulue à un accès tenté par force. Le message d’alarme est immédiatement transmis au PC-client pour l’information du gardien ou pour l’établissement d’un rapport d’alarme.

Il y a plusieurs types différents de nœuds qui assistent le système de gestion de sécurité, parmi eux multiNODE-2, M2000, M2100 et multiNODE-Lite.

Le nombre des lecteurs, etc. qu’un nœud peut commander, dépend du type de nœud. Le M2100 p.ex. est en mesure de gérer jusqu’à 16 lecteurs. Votre système peut facilement être étendu afin de mettre à la disposition plus d’appareils en y connectant des nœuds supplémentaires.

La communication entre un ordinateur et une chaîne de nœuds peut se faire via un lien sériel, à travers un lien de réseau ou par l’emploi d’un modem de connexion. Sinon on peut utiliser un mélange de méthodes. Un ordinateur peut par exemple communiquer avec une chaîne de nœuds en passant par un lien de réseau (LAN), mais il peut y avoir aussi un lien de modem de reprise automatique reliant la chaîne au PC, qui pourrait servir à transmettre des alarmes dans l’événement au cas où le lien de communications de réseau est inopérant.

Les communications sérielles peuvent être améliorées par la connexion d’un nœud final dans la chaîne avec un autre port sur le PC. Si au milieu de l’événement le lien de communications est interrompu, le PC peut communiquer avec les nœuds en passant par le port alternatif.

Une fonction optionnelle est également disponible pour le cryptage de communications afin d’assurer la sécurité de communications entre une chaîne LAN et le PC de contrôle.

Les modems

Grâce aux modems les nœuds se trouvant sur des emplacements éloignés sont capables d’être mis en oeuvre en fournissant les moyens à communiquer par l’intermédiaire de connexions téléphoniques standard. Le gestionnaire de système prérègle les heures auxquelles le PC et les nœuds à distance entrent en communication (à charger localement l’activité mémorisée), d’habitude la nuit.

Dans le but de maintenir la sécurité du système, les alarmes détectées par les nœuds lointains sont immédiatement communiquées au PC-client de contrôle.

Un modem s’emploie également à acheminer automatiquement les alarmes jusqu’à des installations tout à fait indépendantes du système de gestion de sécurité. De cette manière il est possible de transmettre automatiquement les alarmes générées p.ex. sur un site non habité la nuit vers un autre site gardé par un service de sûreté 24 heures sur 24.

Les points de surveillance

Il s’agit-là de détecteurs infra-rouges, de claviers à touches installés à chaque niveau, de contacts de porte ou d’appareils pareils. Ils sont surveillés en permanence, et si une intrusion intervient, le nœud déclenche une réaction prédéterminée sous forme ou d’une alarme sur le PC ou enregistré vidéo numérique sur un ENVS.

Les sorties auxiliaires

Ce sont des unités de sortie telles que des luminaires extérieurs, caméras vidéo et barrières qui sont à mettre en ou hors circuit (ou dont le fonctionnement est préréglé pour une certaine durée) ou par voie de commande manuelle depuis un PC-client ou par voie automatique suivant une commande de déclenchement ou programmées. Une commande programmée peut allumer p.ex. une caméra vidéo à des heures du jour préfixées.

Systèmes de vidéo-surveillance (CCTV) et de vidéo numérique

Le Le système SMS de gestion de la sécurité supporte une large gamme de caméras de télésurveillance et matériel vidéo qui permet:

- De visionner et d'enregistrer les images des caméras de surveillance à partir de chaque client du logiciel SMS.
- De contrôler la fonction panoramique, l'inclinaison et les positions prédéfinies (Fonction PTZ).
- Un contrôle complètement intégré du système ENVS (Edge-of-Network Video Servers). Ces dispositifs qui se connectent directement au réseau permettent d'afficher, d'enregistrer de façon numérique et de visionner des vidéos provenant d'un maximum de quatre caméras vidéo. Des commandes fonctionnelles peuvent être paramétrées pour enregistrer les images des alarmes – les enregistrements sont étiquetés en mentionnant l'alarme déclenchante et peuvent être facilement visionnés. Chaque système ENVS a des points de contrôle et des sorties auxiliaires pour le contrôle d'équipement tel que les lampes des caméras, les pompes de gicleurs de nettoyage et les essuie-glaces.
- L'utilisation de caméras vidéo numériques IP qui se connectent directement au réseau.
- De contrôler les magnétoscopes externe et les caméras connectées.
- Un contrôle manuel ou automatique des contacteurs des caméras de surveillance externes. Les contacteurs de caméra de surveillance externes sont utilisés pour afficher des vidéos en temps réels à partir de n'importe quelle caméra connectée sur un moniteur sélectionné en réponse à une commande manuelle ou automatique

Le logiciel SMS offre des outils efficaces pour le contrôle, la surveillance, l'archivage et le visionnage vidéo. Un système de "vérification vidéo" permet à un gardien de comparer l'image d'un détenteur de carte prise en directe à celle stockée afin d'autoriser ou d'interdire, le cas échéant, l'accès.

La vidéo numérique et d'autres dispositifs de vidéosurveillance sont disponibles avec le module de gestion vidéo numérique.

Panneaux d'intrusion/d'alarme

En plus de ses propres possibilités de contrôle des alarmes avec l'utilisation de points de contrôles, le système SMS offre une intégration avec les panneaux d'alarme et d'intrusion à travers le module optionnel d'interface anti-intrusion. Ceci permet le contrôle complet des alarmes et la création de rapports à partir d'une interface utilisateur centralisée.

Les commandes à déclenchement offrent un contrôle automatique des équipements externes si une alarme est déclenchée.

Système d'interphone

Le module optionnel de gestion des interphones offre une interface graphique facile à utiliser pour gérer les appels des interphones et y répondre. Les opérateurs peuvent communiquer avec les personnes qui utilisent l'interphone en utilisant de simples boutons d'écrans. Un bouton de **Commande** permet à une barrière ou une porte associée avec l'interphone sélectionné d'être ouverte.

Les types de produit

Il y a quatre types différents du système de gestion de sécurité: Lite Edition, Professional Edition, Enterprise Edition and Global Edition.

Les systèmes Lite Edition

Lite Edition est un véritable système de client/serveur, avec une configuration maximum de jusqu'à 16 lecteurs, 1000 cartes et 3 clients. Si besoin est, l'ensemble du logiciel peut être installé sur un seul PC.

Le système Lite Edition utilise les banques de données du serveur SQL qui sont gérées par Microsoft Data Engine (MSDE). Grâce à sa capacité maximum de 2 GB pour les banques de données, le MSDE a été conçu et optimisé pour l'usage sur des systèmes de taille moins importante.

Les systèmes Professional Edition

Professional Edition est un système qui s'appuie sur les qualités du système Lite Edition pour fournir une configuration maximum de jusqu'à 512 lecteurs et 9 clients en fonction du paquet fourni compte tenu d'une quantité illimitée de cartes.

Les systèmes Enterprise Edition

Ce système réunit toutes les caractéristiques du système Professional Edition, utilise pourtant le système complet de gestion du serveur Microsoft SQL pour les banques de données relationnelles qui répond aux exigences de grand débit et de capacité modulable. Cette configuration permet l'expansion illimitée de systèmes de grande taille.

Les systèmes Global Edition

Ce système s'appuie sur celui d'Enterprise Edition pour mettre à la disposition des possibilités élargies pour la gestion à distance de systèmes multiples qui se trouvent répartis sur un nombre de sites géographiquement distants l'un de l'autre.

Le système Global Edition assiste les „Global Clients" (Cf. figure 1.2). Chaque „Global Client" peut avoir une connexion avec n'importe quel système régional et s'y inscrire comme s'il s'agissait d'un client local de ce même site. Ceci permet une vraie gestion des sites à distance, tout en rendant possible l'entier accès aux rapports d'événements (en fonction des autorisations d'utilisateur), à la gestion des cartes et au contrôle des lecteurs, portes et points de surveillance.

Au choix, les Global Clients peuvent également être pourvus des capacités du traitement des alarmes. C'est ainsi que les sièges sociaux ou systèmes régionaux peuvent communiquer avec le „Global Client" pour centraliser l'enregistrement et la gestion des alarmes. Ces dernières peuvent être acheminées vers les „Global Clients" à des heures du jour spécifiées, p.ex. en-dehors des heures d'ouverture.

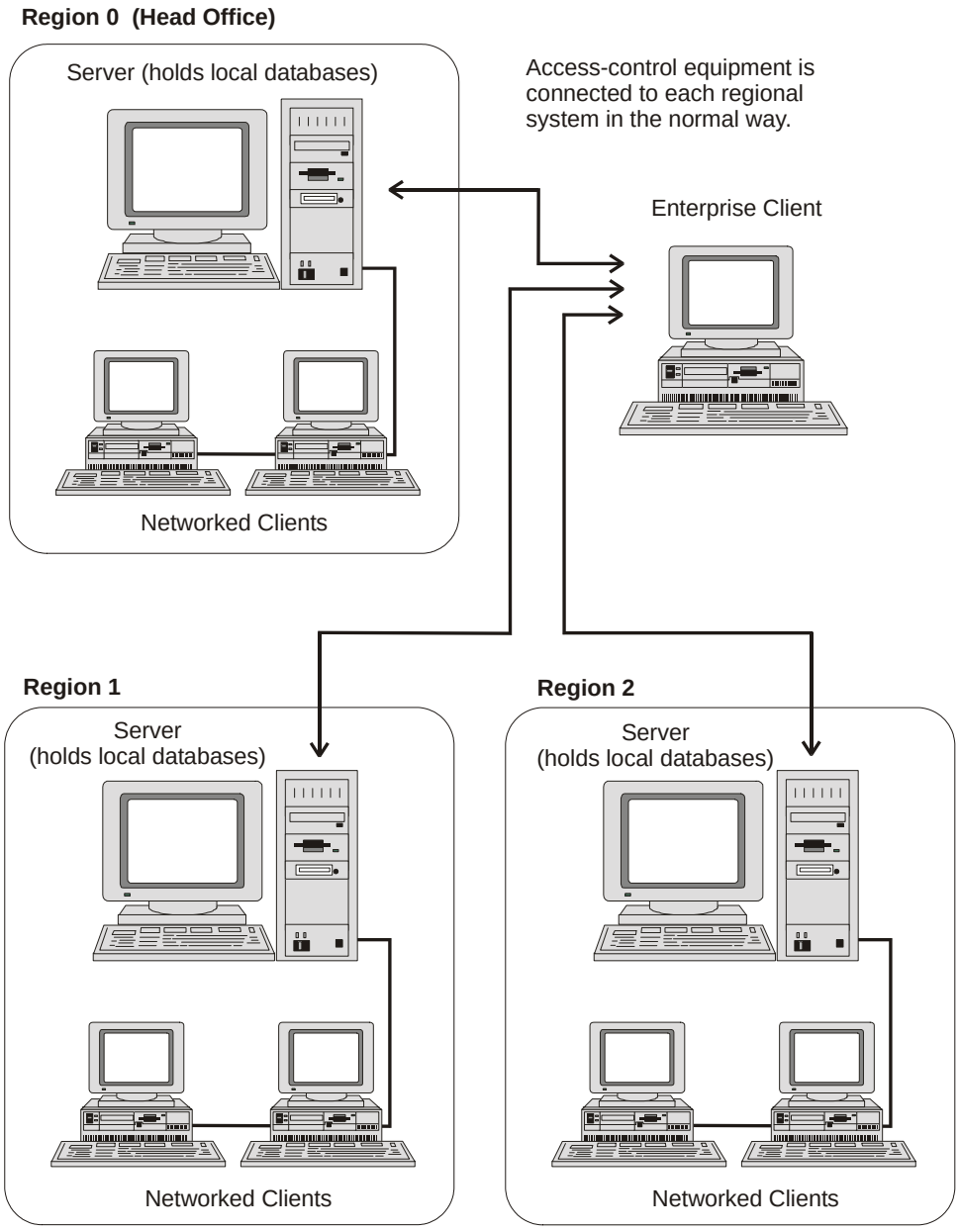


Figure 1.2: Le système Global Edition avec des „Global Clients“

Une autre option du système Global Edition soutient la gestion centrale de cartes (Cf. figure 1.3). Ceci permet de centraliser la saisie des détenteurs de cartes, de les affecter à un ou plusieurs systèmes régionaux et de les faire importer automatiquement par tous les sites possibles.

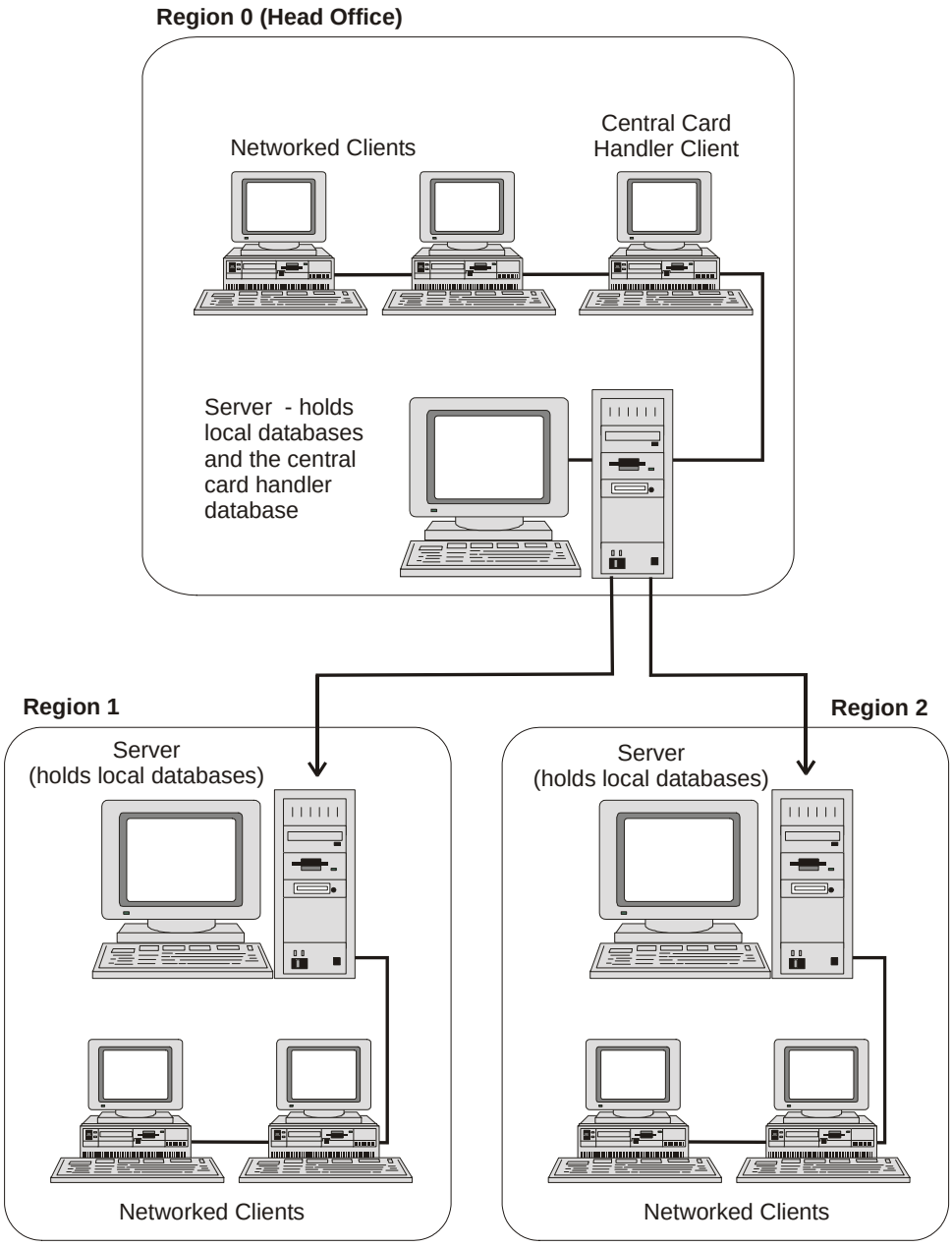


Figure 1.3: L'exemple du système Global Edition avec le traitement central de cartes

Le traitement central de cartes ne permet pas seulement une meilleure organisation de sites multiples du point de vue gestion centrale des cartes, elle est aussi la solution idéale pour le cas où des personnes demandent l'accès à plus d'un site, car il faut une seule opération pour ajouter des cartes à tous les points respectifs.

L'architecture du système Global Edition crée la résistance ultime pour les applications sur des sites multiples, car s'il y a une défaillance survenue sur un lien de réseau d'entreprise il est toujours possible que les systèmes régionaux autonomes continueront à fonctionner à cent pour cent au niveau local.

Chapitre 2: Comment bien démarrer

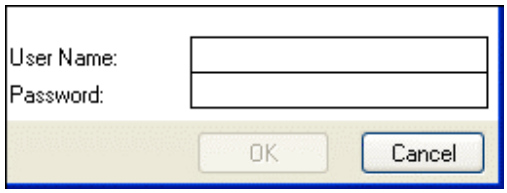
Ouvrir le logiciel de gestion de sécurité (SMS)

Pour démarrer le logiciel de gestion de sécurité:

1. Double-clic sur l'icône du dessus de l'écran Windows:

   Sélectionnez alternativement **Start/Programs/Security Management System/Security Management System** (Démarrer/Programmes/Système de gestion de sécurité/Système de gestion de sécurité).

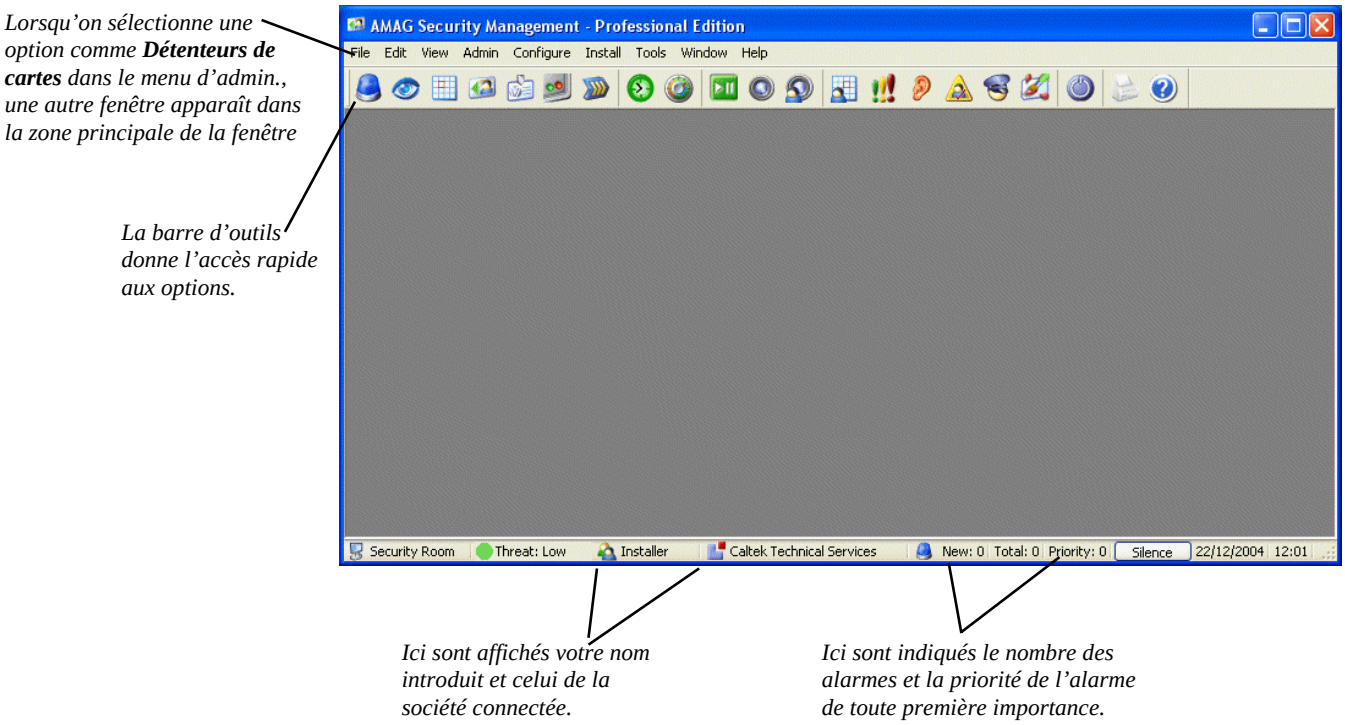
2. Vous êtes alors invité à entrer en connexion, comme présenté ci-dessous. Afin d'accéder aux fenêtres du logiciel de gestion de sécurité, il faut introduire le nom d'utilisateur et le mot de passe accordés. L'accès est seulement autorisé, si leur validité est reconnue.



Une fois effectué l'opération de demande de connexion, on peut changer le mot de passe par l'option **Set Password** dans le menu d'outils.

L'option **Logoff** (sortir) dans le menu de fichier permet de terminer la session et de retourner à la fenêtre „log in". Il est à signaler que le système peut automatiquement terminer la session (défaut 15 minutes), si l'on n'a pas utilisé l'ordinateur pour une durée prédéterminée.

Après une opération réussie de „log in" la fenêtre de gestion de sécurité s'ouvre avec en haut le menu d'options et la barre d'outils comme il est présenté dans la figure ci-après.


Lorsqu'on sélectionne une option comme **Détenteurs de cartes** dans le menu d'admin., une autre fenêtre apparaît dans la zone principale de la fenêtre
La barre d'outils donne l'accès rapide aux options.
AMAG Security Management - Professional Edition
File Edit View Admin Configure Install Tools Window Help
Security Room
Threat: Low
Installer
Caltek Technical Services
New: 0 Total: 0 Priority: 0
Silence
22/12/2004 12:01
Ici sont affichés votre nom introduit et celui de la société connectée.
Ici sont indiqués le nombre des alarmes et la priorité de l'alarme de toute première importance.

Au sujet de l'interface utilisateur

Le logiciel se sert de l'interface utilisateur graphique de Microsoft Windows, grâce à laquelle le produit est facile à apprendre et à utiliser.

L'interface utilisateur se compose d'un nombre de fenêtres organisées logiquement qui permettent l'accès depuis une seule barre de menu ou depuis des barres d'outils. Les barres d'outils peuvent être déplacées dans n'importe quelle position à l'intérieur de la fenêtre de gestion de sécurité. Les barres d'outils adaptées aux besoins de l'utilisateur peuvent également être déterminées pour donner accès à vos écrans favoris.

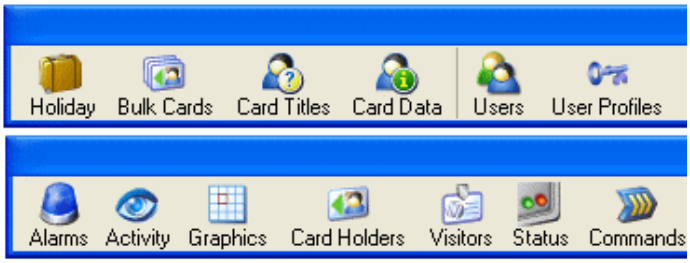
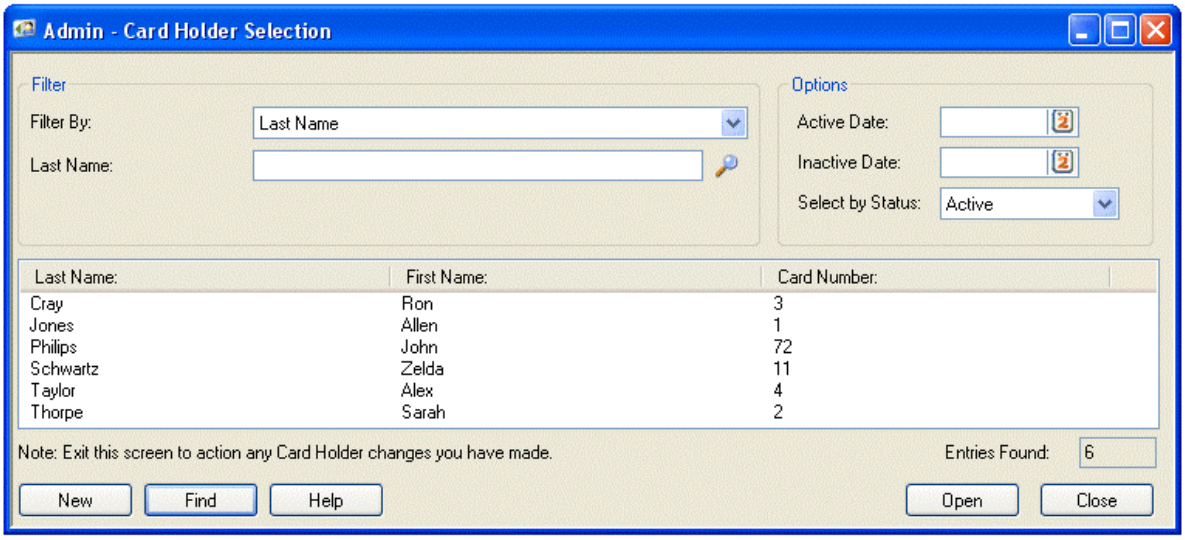


Figure 1.2: Des exemples de barres d'outils

Le logiciel utilise des attributs comme des icônes, des barres d'outils, des vues d'arbre et les techniques de glisser-déposer afin de conférer à l'interface utilisateur un caractère d'intuition et de maniabilité. Toutefois si vous avez besoin d'informations d'aide contextuelle en ligne une aide générale en ligne depuis toutes les fenêtres.

Les fenêtres de sélection et de définition

Beaucoup d'options des menus d'administration et de configuration, p.ex. l'option de groupes de lecteurs, affichent deux fenêtres: la fenêtre „Sélection" (p.ex. la fenêtre de sélection du détenteur de carte) et la fenêtre „Définition" (p.ex. la fenêtre de définition du détenteur de carte). La fenêtre de sélection est celle qui apparaît lorsqu'on sélectionne d'abord l'option. Exemple:



La fenêtre contient une option **Find** (rechercher), qui vous aide à trouver tous les éléments existants (p.ex. les détenteurs de cartes existants). Les éléments trouvés sont regroupés dans une liste sur l'écran, souvent avec d'autres informations dans ce contexte.

Si vous désirez pouvoir sélectionner certains éléments listés, vous avez le choix de les filtrer au moyen des options en haut de l'écran. En sélectionnant par **Find** (rechercher), seuls ces éléments sont affichés que le filtre a sortis.

Si l'on sélectionne un des éléments listés et si on clique ensuite sur **Open** (ouvrir), la fenêtre de définition s'ouvre, dans laquelle on peut faire le suivant:

- Visualiser ou modifier les détails de l'élément sélectionné. A noter: On peut seulement y avoir accès si une autre personne du réseau est en train de visualiser ou de modifier l'élément.
- Appliquer l'option **Delete** pour effacer entièrement l'élément dans le système.
- Appliquer l'option **Copy** pour copier les détails d'un élément afin de créer un nouvel élément.

Alternativement, on peut sélectionner l'option **New** pour créer un nouvel élément (p.ex. mettre en place un nouveau détenteur de carte).

Au sujet de vos droits d'utilisateur

Le nom d'utilisateur entré décide des options qui sont à votre disposition et de ce qui est permis de faire dans les fenêtres. Exemple: Vous avez le droit sans restriction de changer les informations dans certaines fenêtres, tandis que vous n'êtes autorisé qu'à les visualiser dans d'autres fenêtres. Des renseignements plus détaillés sur les possibilités des utilisateurs sont définis à la page 9-1.

Qu’est-ce qu’il faut faire ensuite?

Avant de commencer en œuvre le logiciel de SMS il vous faut vérifier si votre matériel de système a été configuré correctement et si les options sont contenues dans le menu d’installation. Ce guide utilisateur part du principe que ces tâches ont été complétées pour vous par un installateur et inclut de préparer:

- les PC-clients prévus à être mis en oeuvre
- les ports de PC que le matériel de gestion de sécurité aura à connecter
- les chaînes de nœuds
- les nœuds, lecteurs, points de surveillance, caméras CCTV, enregistreurs vidéo numériques, etc. au sein de votre système

Une fois que ces tâches sont complétées, vous pouvez utiliser ce Guide d'utilisation pour faire plus ample connaissance avec le logiciel SMS. Vous apprendrez comment paramétrer des: Détenteurs les détenteurs de cartes et des droits.

- les détenteurs de cartescréer, imprimer et encoder les badges ID (ou cartes pour le contrôle d’accès); Cf. Chapitre 4.
- utiliser le système pour la gestion des visiteurs; Cf. Chapitre 5.
- découvrir comment utiliser et contrôler les caméras CCTV et les enregistreurs vidéo numériques; Cf. Chapitre 6.
- installer et mettre en œuvre les caractéristiques de la surveillance des alarmes; Cf. Chapitre 7.
- installer et générer les rapports; Cf. Chapitre 8.
- Utiliser d'autres dispositifs importants - Chapitre 9;

D’autres modules optionnels sont décrits dans des manuels séparés; Cf. page iv.

Chapitre 3: La gestion des cartes

Ce chapitre décrit comment installer les détenteurs de cartes et définir les droits d'accès.

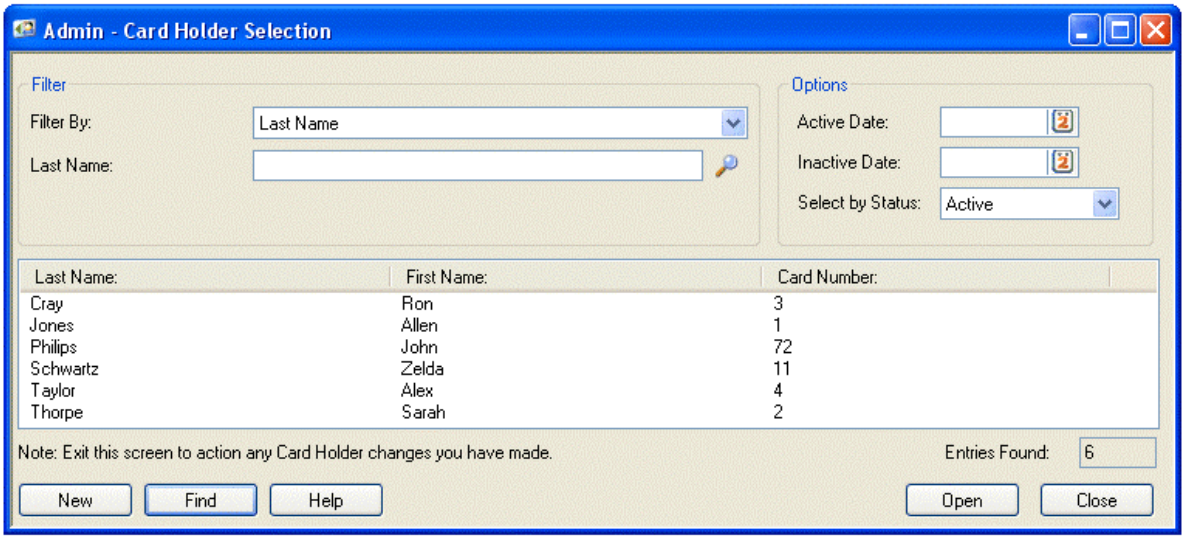
Au sujet de la fenêtre des détenteurs de cartes

Dans la fenêtre Détenteur de carte, qui apparaît lorsqu'on sélectionne l'option **Card Holder** du menu d'administration, on ajoute les détails de chaque personne qui demande une carte de contrôle d'accès ou un badge d'identité (sauf ces visiteurs qui sont déjà installés dans la fenêtre Admin/Visitors). En utilisant la fenêtre des détenteurs de cartes on peut:

- entrer les coordonnées du détenteur de carte, p.ex. son nom, le numéro de carte et des détails personnels
- spécifier les droits d'accès pour un détenteur de carte, c'est-à-dire les portes, auxquelles le détenteur de carte peut avoir accès, et les heures autorisées à y accéder
- prendre une photo et la signature qui sont à inclure dans le badge imprimé
- imprimer et encoder les cartes
- saisir les données biométriques, telles que les empreintes digitales, que l'on peut encoder sur les cartes à mémoire à présenter aux lecteurs d'accès haute sûreté spécialement prévus à cette fin

Créer ou trouver un détenteur de carte

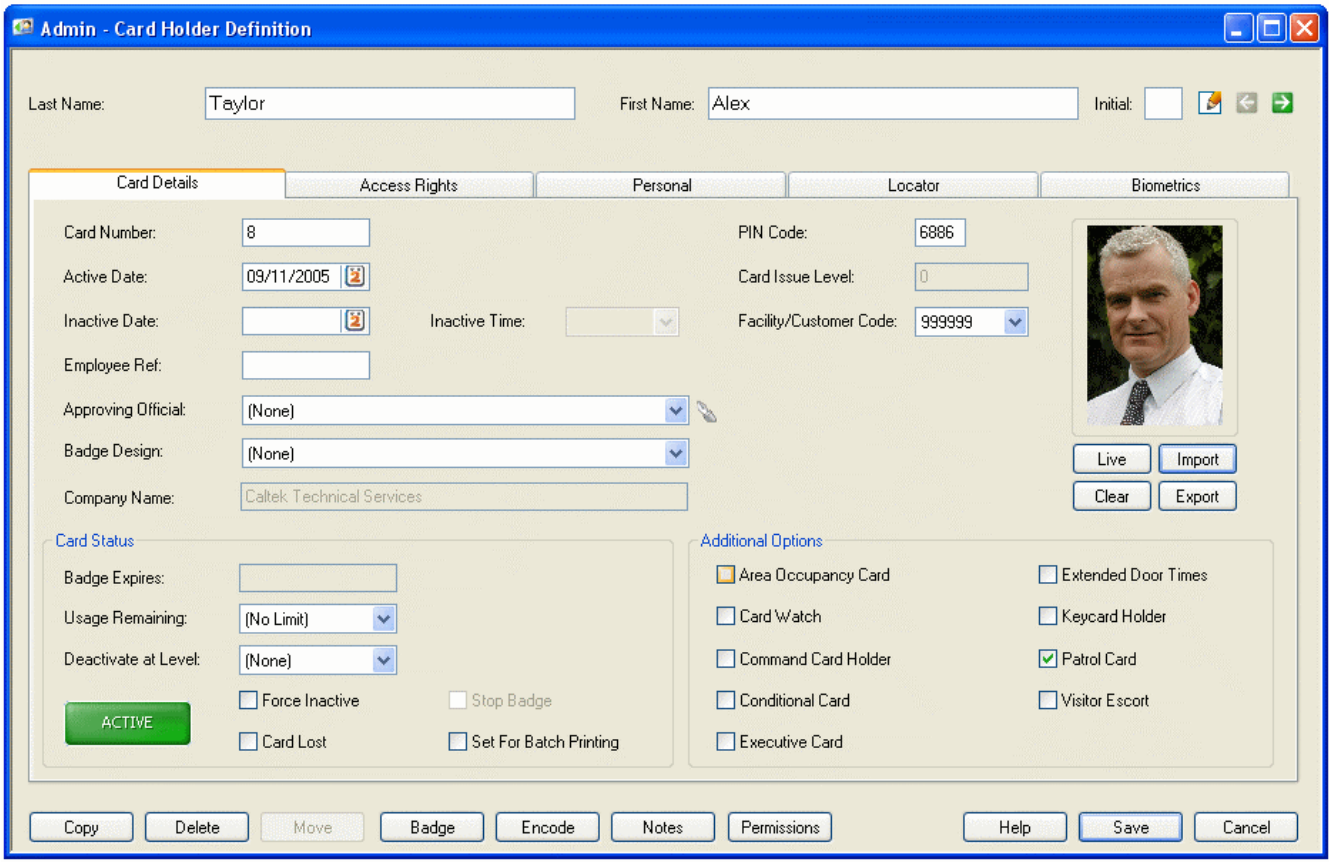
Lorsqu'on sélectionne l'option **Admin/Card Holder**, la fenêtre de sélection apparaît d'abord:



Dans cette fenêtre on peut:

- cliquer sur **Find** pour trouver un détenteur de carte existant, ensuite cliquer sur **Open** pour visualiser ou modifier les éléments de la carte du détenteur.
- cliquer sur **New** pour créer les éléments pour un nouveau détenteur de carte.

Dans l'exemple suivant ont été ouverts les éléments d'Alex Taylor (un détenteur de carte existant) à partir de la fenêtre de sélection.



La fenêtre de définition des détenteurs de cartes (Card Holder Definition) contient un nombre d'onglets:

- **L'onglet de détails de carte (Card Details)** – permet de prendre la photo du détenteur de carte et d'introduire les informations, p.ex. des données comme la validité d'une carte, la conception du badge et certains privilèges dont vous voulez doter la carte. Cf. à la page 3-4.
- **L'onglet de droits d'accès (Access Rights)** – spécifie ces portes, par lesquelles le détenteur de carte a le droit d'entrer et de sortir. **Cf.** Error! Reference source not found. **à la page Error! Bookmark not defined.**.
- **L'onglet de personnel (Personal tab)**– permet de spécifier les informations personnelles concernant les détenteurs de carte. Cf. ***Error! Reference source not found.*** à la page **Error! Bookmark not defined.**.
- **L'onglet de localisation (Locator)** – pour trouver la position d'un détenteur de carte à un moment donné. Cf. ***Error! Reference source not found.*** à la page **Error! Bookmark not defined.**.

- **L'onglet Biometrics** – permet de saisir les données biométriques comme les empreintes digitales et la signature du détenteur de carte. Cf. Chapitre 4.

L'accès de certains onglets dépend des permissions attribuées à l'utilisateur.

Dans les passages suivants sont décrites les caractéristiques principales de la fenêtre des détenteurs de cartes. Pour de plus amples informations veuillez vous référer au programme d'aide *Online Hel*p.

Le nom de famille, le prénom et l'initiale

Pour chaque détenteur d'une carte il faut spécifier ses noms suivant **nom de famille (Last Name)** et **prénom (First Name)**. Si vous voulez, vous pouvez remplir le champ **Initial** en y mettant la première lettre (l'initiale donc) p.ex. du deuxième prénom du détenteur de carte.

Si possible, on devrait se rassurer que ces trois champs identifient le nom unique d'un détenteur de carte, sinon on trouverait des rapports, etc. où sont confondues deux personnes du même nom.

Le numéro de carte

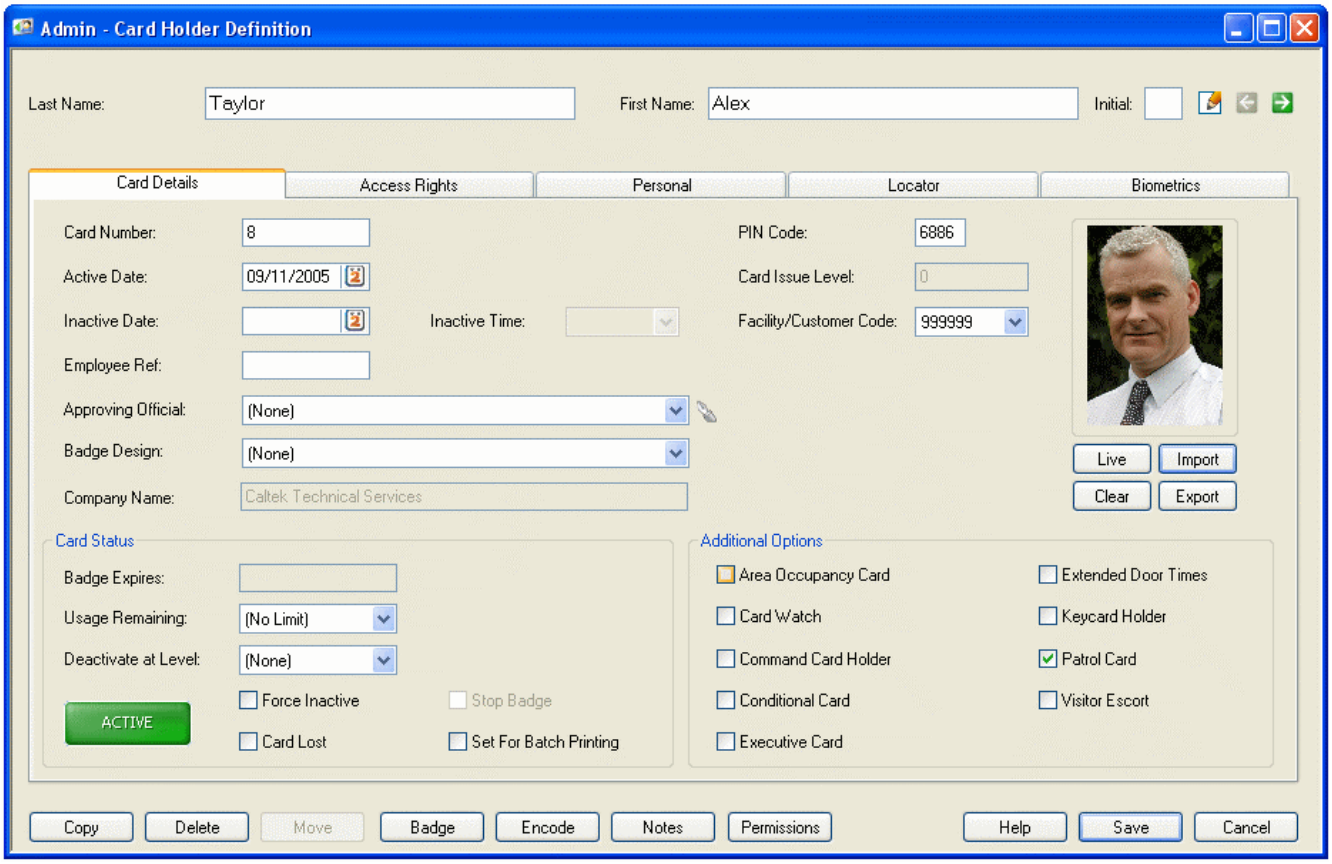
Le n° de carte (**Card Number)** devrait normalement exister une seule fois. Si l'on présente la carte au contrôle d'accès, le numéro de carte doit correspondre à celui de la carte distribuée au détenteur.

Si le champ **Card Number** est laissé libre, lorsqu'on définit les éléments d'un nouveau détenteur de carte, un numéro est automatiquement attribué après qu'on a sélectionné **Save** (sauvegarder), le n° de carte automatique **(Auto Card Number)** apparaissant dans la fenêtre Configure/Preferences/System. Si pourtant on ne sélectionne pas **Auto Card Number** il y a un zéro qui apparaît comme n° de carte (on peut introduire le numéro correct ultérieurement).

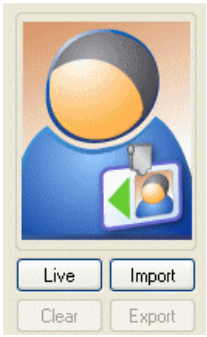
Si vous utilisez une carte à bande magnétique et si vous disposez d'une unité d'encodage appropriée, vous pouvez mettre un numéro codé sur la carte en recourant à la fenêtre Tools/Encode Cards (outils/encodage de cartes) ou en imprimant le badge. Si vous vous servez de cartes à mémoire vous pouvez appuyez sur le bouton **Encode** (encodage) dans la fenêtre des détenteurs de cartes aux fins d'encodage de la carte.

Créer les détails de cartes

Ce paragraphe décrit les caractéristiques principales de l'onglet des détails de carte dans la fenêtre Admin/Card Holder.



La photo du détenteur de carte



Si cette icône est affiché sur la droite de l'onglet Card Details, elle indique que l'image du détenteur de carte n'a pas encore été saisie. Une photo peut être demandée pour le badge du détenteur de carte (Cf. page 4-3). Une fois saisie, la photo réelle du détenteur de carte remplace l'icône.

L'onglet offre deux méthodes alternatives à prendre la photo de la personne:

- **Live** – En cliquant sur ce bouton, l'image du détenteur de carte est directement prise par une caméra connectée au PC.
- **Import** – En cliquant sur ce bouton, l'image enregistrée du détenteur de carte est importée (p.ex. prise par une caméra numérique).

Les dates actives et inactives

On utilise **Active Date** et **Inactive Date** pour spécifier la période pendant laquelle la carte peut être utilisée pour avoir le droit d'accès (les portes et heures autorisées sont définies dans l'onglet des

droits d'accès). Une carte ne peut pas être acceptée durant la période de son **Inactive Date** à partir de minuit, nonobstant les droits d'accès.

Le code PIN

L'option **PIN Code** permet de spécifier un code d'identification personnelle (PIN) pour le détenteur de carte. Ceci est d'importance pour tout détenteur de carte utilisant les lecteurs de carte et de PIN, l'accès ne pouvant pas être libéré avant que le détenteur de carte n'ait présenté la carte resp. entré son PIN correct.

C'est par des commandes (Cf. page **Error! Bookmark not defined.**) que l'on peut à n'importe quel moment régler tout lecteur ou en mode de CARTE SEULE (card-only) ou en mode de CARTE ET PIN (card-and-PIN). Si un lecteur est mis en mode de carte seule il n'est pas nécessaire d'introduire le PIN, ce qui peut être sensé pendant les heures d'ouverture très fréquentées dans la journée.

Un détenteur de carte peut également utiliser le PIN pour créer une alarme/un événement „forcés" („duress" alarm/event), en mettant un zéro devant le PIN sans entrer le dernier chiffre. L'alarme/l'événement signalent que le détenteur de carte a forcé l'accès. Le mode „forcé" peut être mis en ou hors service sur chaque lecteur.

Le code de bâtiment/client (Facility/Customer code)

Certaines cartes comprennent un code client (connu aussi comme „facility code"). Il identifie la société du détenteur de carte. Vous avez à choisir le code dans le menu **Facility/Customer Code**. Les codes du menu sont définis dans la fenêtre Facility/Customer Codes du menu de configuration.

La conception des badges et leur expiration

Vous pouvez vous servir du menu **Badge Design** pour sélectionner le format du badge pour le détenteur de carte (Cf. page **Error! Bookmark not defined.**).

Si la conception du badge a une échéance, la date d'expiration est affichée sous **Badge Expires**. Si le badge est utilisé comme une carte de contrôle d'accès, on ne pourra plus avoir accès une fois cette date est expirée.

Les options de carte supplémentaires

On peut se servir des cases de contrôle dans la zone des options de carte supplémentaires (**Additional Card Options)** pour déterminer les privilèges additionnels du détenteur de carte, p.ex.:

- **Executive Card** (carte générale) – Le détenteur d'une carte générale n'a pas besoin d'entrer un PIN aux lecteurs mis en mode combiné de carte et PIN.
- **Extended Door Times** (temps de porte étendus) – C'est utile pour les détenteurs de carte handicapés ou étant dans l'embarras ne pas pouvoir ouvrir une porte ni pouvoir y passer aussi rapidement que c'est normalement nécessaire. Si vous sélectionnez l'option, le système utilise le temps de porte étendus (se trouvant dans la fenêtre Admin/Door Timing) à chaque fois que ce détenteur de carte demande l'accès.
- **Command Card Holder** (détenteur d'une carte de commande) – C'est ainsi que le détenteur de carte peut générer des messages de commande aux lecteurs à clavier numérique. Les messages peuvent servir à activer ou désactiver les systèmes d'alarme d'intrusion ou à allumer ou éteindre des lumières par l'emploi de commandes de déclenchement. Les commandes données par carte permettent aussi aux utilisateurs de changer leur PIN ou les temps d'ouverture des portes.

L'état du détenteur de carte

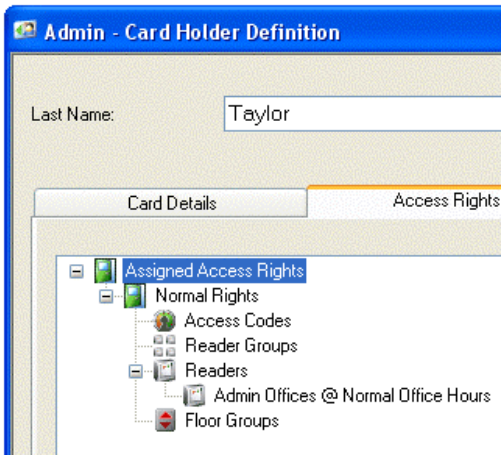
Le **Card Holder Status** indique l'état d'une carte à un moment donné, de sorte que l'on puisse le changer. Exemple, la sélection de **Card Lost** (carte perdue), ce fait supposé, est utile, si la carte a été perdue ou volée. Car si quelqu'un essaie de s'en servir, l'alarme/l'événement de „Lost Card" se déclenchent et l'accès n'est pas accordé.

Active – c'est l'état courant d'une carte avec laquelle on peut passer normalement.

L'état d'expiration peut intervenir automatiquement, si la carte n'est pas utilisée pour une durée spécifiée (peut-être parce que le détenteur de carte ne travaille plus pour votre société). La durée de cette période peut être spécifiée dans la fenêtre Configure/Preferences/System.

Créer et accorder les droits d'accès

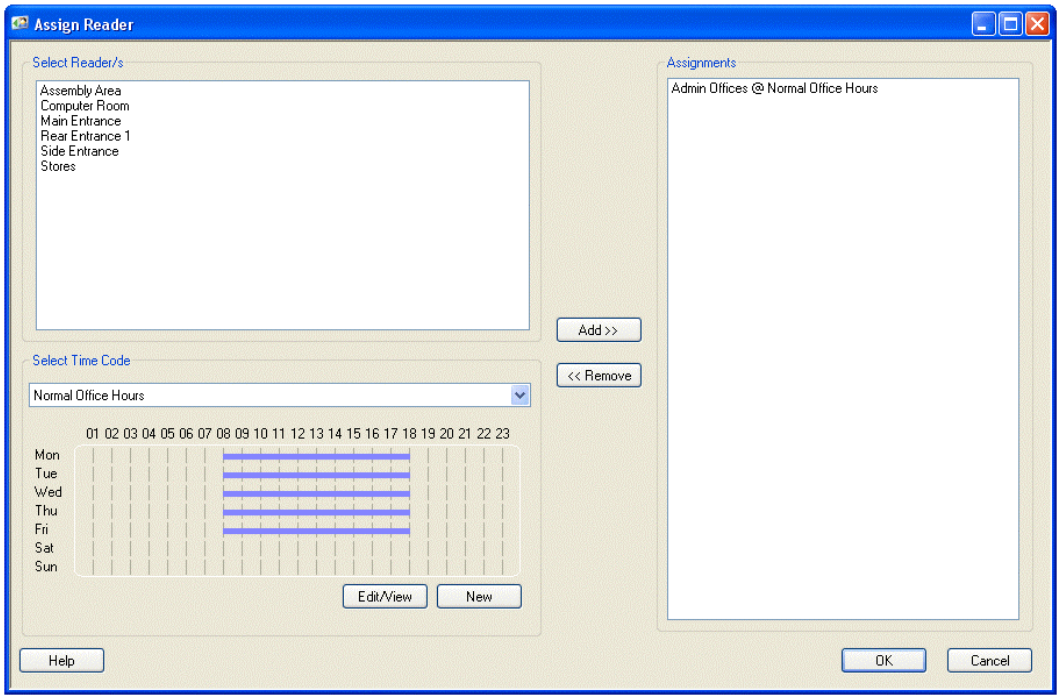
Les droits d'accès d'un détenteur de carte qui peuvent être spécifiés dans l'onglet des droits d'accès dans la fenêtre des détenteurs de carte, déterminent à quelle partie du bâtiment une personne concernée peut avoir accès à quelle heure. Exemple:



Les droits d'accès accordés à un détenteur de carte peuvent comprendre des droits normaux et étendus, ce qui est affiché dans une vue d'arbre graphique. On peut étendre les branches d'arbre pour regarder leurs contenus de la manière connue. Les droits normaux sont les droits d'accès standard consentis au détenteur de carte. Le niveau hiérarchique le plus élevé de cette branche est toujours affiché dans la présentation d'arbre.

Les droits étendus sont utilisés afin de remplacer les droits d'accès normaux dans des délais spécifiés. Par exemple, si le détenteur de carte a à faire temporairement dans un autre bureau ou bâtiment, les droits étendus s'appliquent à de nouveaux droits d'accès accordés pour les dates respectives. Si les droits étendus ne sont pas mis, on peut sélectionner **Show All** (afficher tout) pour introduire les droits étendus.

On peut attribuer les droits d'accès p.ex. en sélectionnant **Readers** (lecteurs), ensuite **Assign** (assigner). Dans ce cas, le dialogue d'Assign Reader s'affiche:



Dans le dialogue d'Assign Reader, on choisit un ou plusieurs lecteurs parmi ceux de la liste du coin gauche en haut, auxquels le détenteur de carte a le droit d'accéder. Il faut en plus choisir un code de temps **(time code)** (Cf. page 3-8), qui restreint l'accès au lecteur à des heures spécifiées de la journée. L'exemple ci-dessus démontre dans la zone droite que le lecteur à l'entrée principale a été mis au code de temps "Normal Office Hours" (heures de bureau régulières). Le schéma en bas à gauche indique que le code de temps des heures d'ouverture régulières a été spécifié de lundi à vendredi entre 8 et 18 heures, ce qui restreint le passage du lecteur „Entrée principale" à ces heures fixées.

Outre les lecteurs, les onglets de droits d'accès permettent de les introduire compte tenu des inscriptions ci-après:

- **Reader groups** (groupes de lecteurs) – Un groupe de lecteurs réunit un ou plusieurs lecteurs, tels qu'ils sont introduits dans la fenêtre Admin/Group/Readers. Grâce aux groupes de lecteurs on peut accorder d'une manière rapide et facile l'accès par l'intermédiaire de plusieurs lecteurs.

  Normalement les employés qui travaillent dans le même bureau, passent par le même lecteur. Les groupes de lecteurs réduisent donc les dépenses de travail pour l'attribution des droits d'accès aux employés.

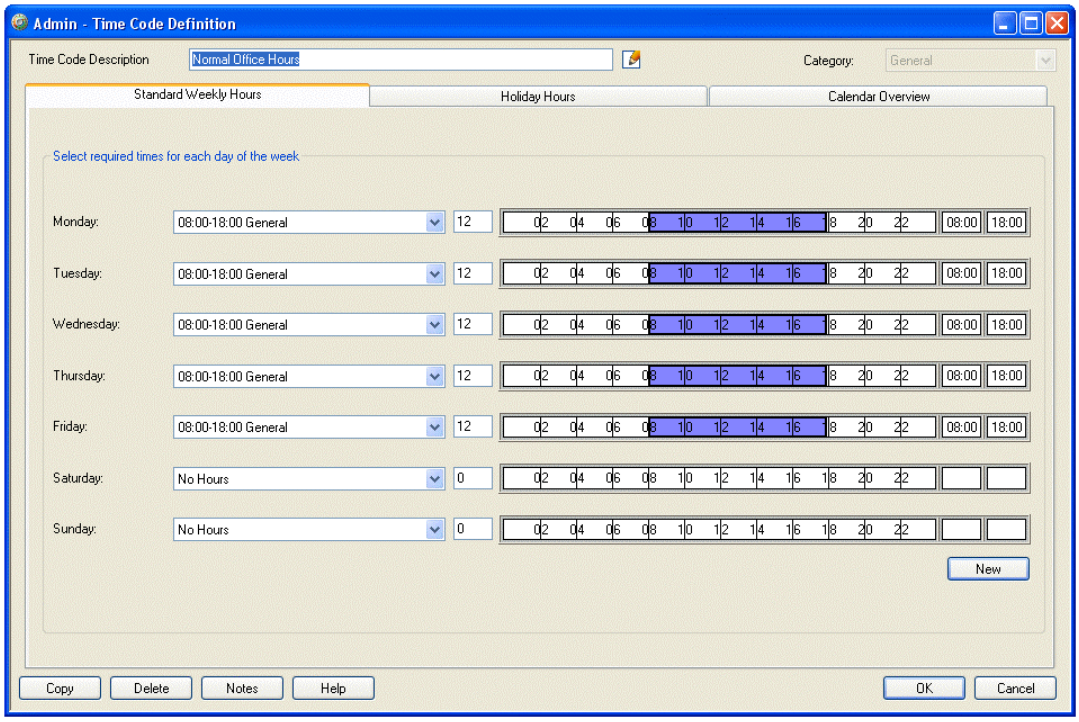
- **Floor groups** (groupes d'étages) – Un groupe d'étages réunit un ou plusieurs étages d'ascenseur, tels qu'ils sont introduits dans la fenêtre Admin/Group/Floor/Output. On en a besoin si l'on veut restreindre les étages qui peuvent être choisis sur un tableau de contrôle d'ascenseur. Exemple: Certains employés nécessitent l'accès aux étages 1 à 10, il y en a d'autres qui ont seulement besoin d'accéder aux étages 1 et 2.

- **Access codes** (codes d'accès) – Un code d'accès est une série de droits d'accès prédéfinie et introduite dans la fenêtre Admin/Group/Access Codes. Un code d'accès peut comprendre une collection de droits d'accès à des lecteurs, des groupes de lecteurs et des groupes d'étages. Les codes d'accès permettent d'accorder en une seule et simple opération l'accès d'un détenteur de carte à tous ces groupes.

Les codes d’accès sont particulièrement utiles dans le cas où l’on veut accorder les mêmes droits d’accès à plus d’une personne. Exemple: On peut établir un code d’accès dit „Admin Staff“ qui contient tous les droits d’accès nécessaires pour les détenteurs de carte travaillant dans l’Administration.

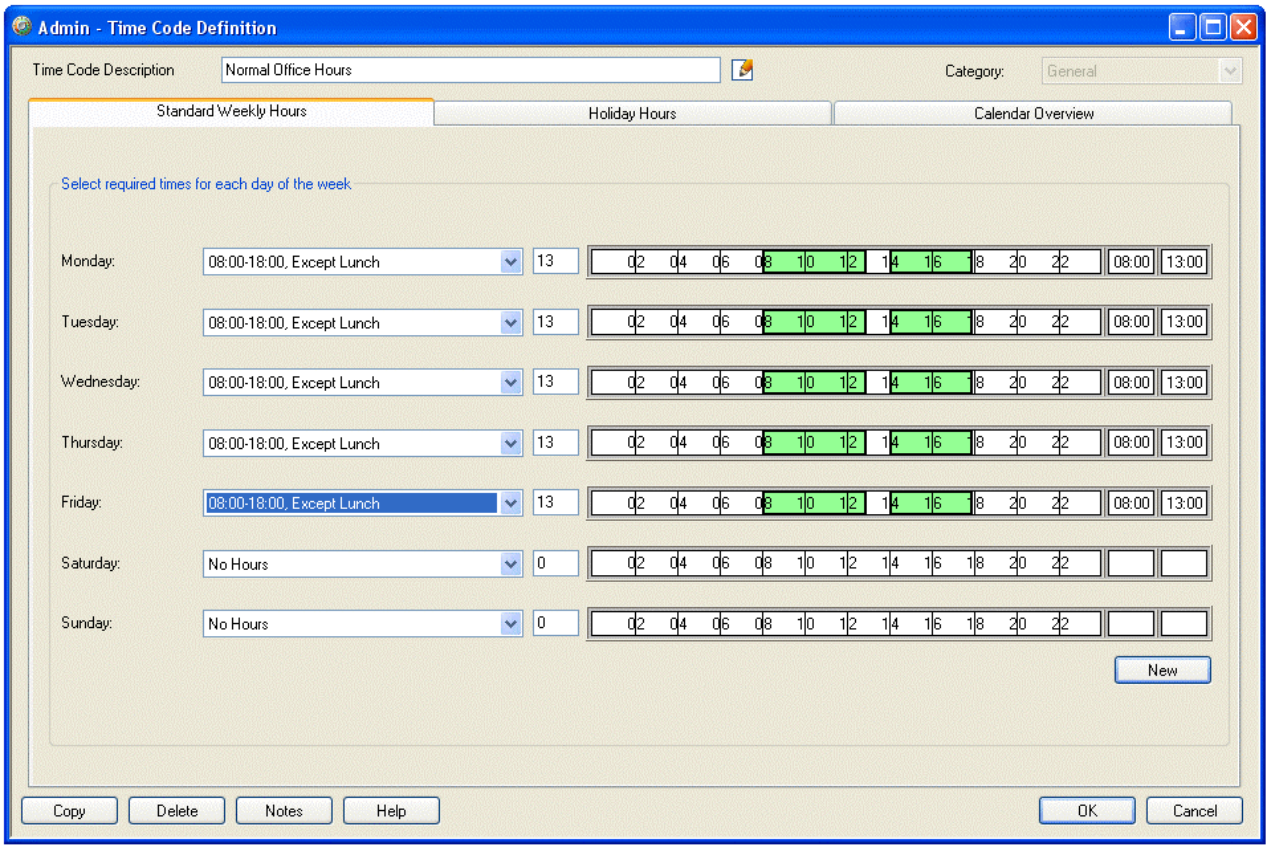
Définir les codes de temps et les heures

On peut définir les codes de temps en recourant à la fenêtre Admin/Times/Time Codes:



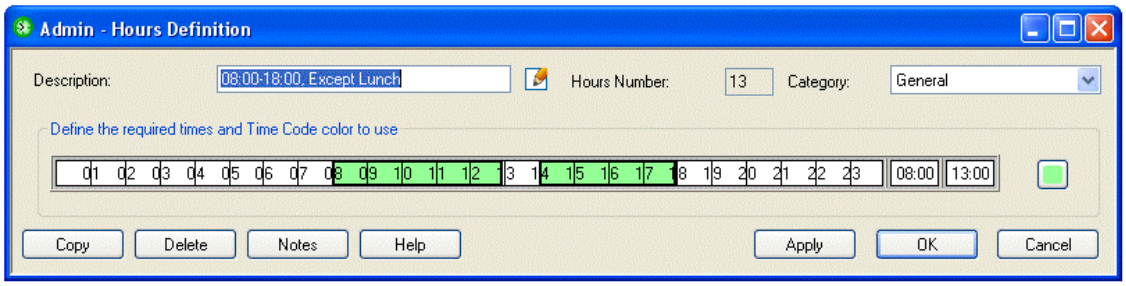
En vous vous servant des listes du menu déroulant dans l’onglet Standard Weekly Hours, vous sélectionnez "hours definition" ce qui est à utiliser pour chaque jour de la semaine. Pour l’exemple ci-haut on avait sélectionné le suivant pour chaque jour ouvrable "08:00-18:00 General", ce qui signifie que l’accès est permis entre 8h00 et 18h00.

En cas de défaut, un chiffre de "hours definition" s’introduit automatiquement pendant l’installation du logiciel, y compris "08:00-18:00 General". Une définition des heures comprend des intervalles de une ou plusieurs fois, elle détermine quand les gens sont autorisés à accéder. Pour l’exemple suivant on a sélectionné la définition des heures "08:00-18:00 Except Lunch", comprenant deux intervalles:



Il est possible d'y avoir un maximum de dix intervalles différents par code de temps.

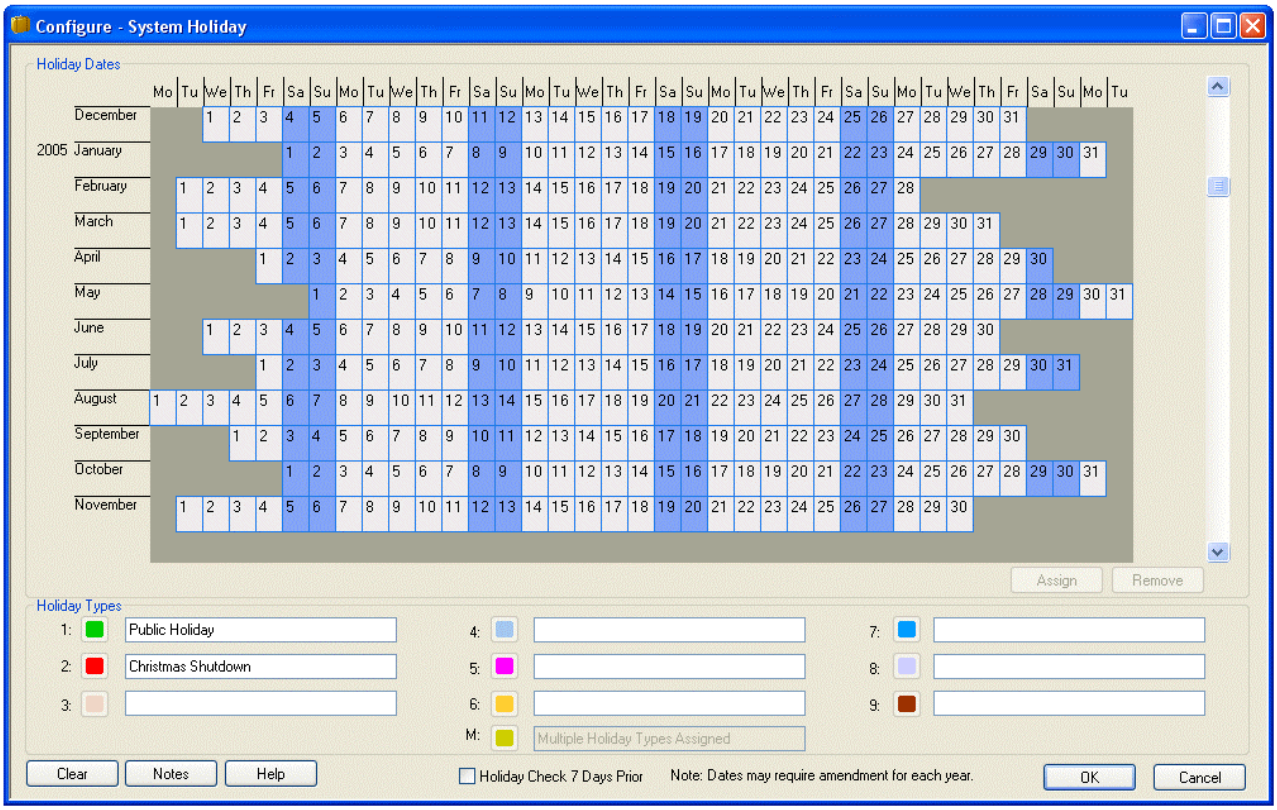
On peut ajouter ou modifier des définitions des heures dans la fenêtre Admin/Times/Hours. Exemple:



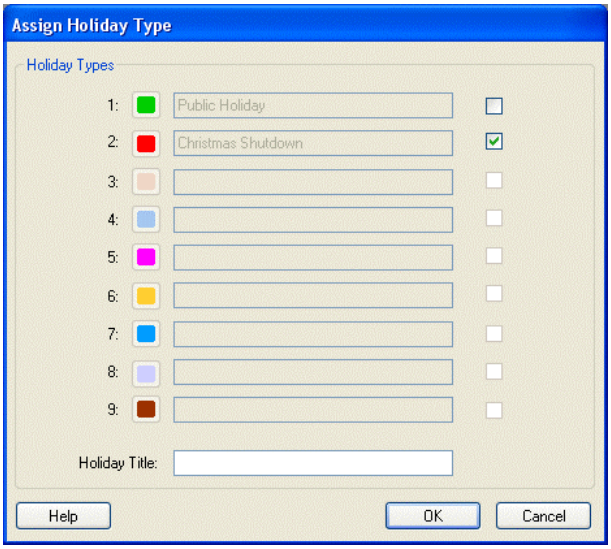
Nota: Les codes de temps (donc les définitions des heures) sont à mettre en œuvre au moment de l'installation des droits d'accès, des commandes de déclenchement ou programmées. On peut se servir du menu déroulant **Category** s'ouvrant dans le coin en haut à droite de "Hours Definition" et de la fenêtre "Time Code Definition" pour restreindre l'usage des titres offerts. Exemple: Lorsqu'on sélectionne **Access Right** il est seulement possible de mettre le code de temps ou la définition des heures au moment de l'installation des droits d'accès. L'installation de défaut se fait par **General**, ce qui permet l'usage illimité.

Définir les jours fériés

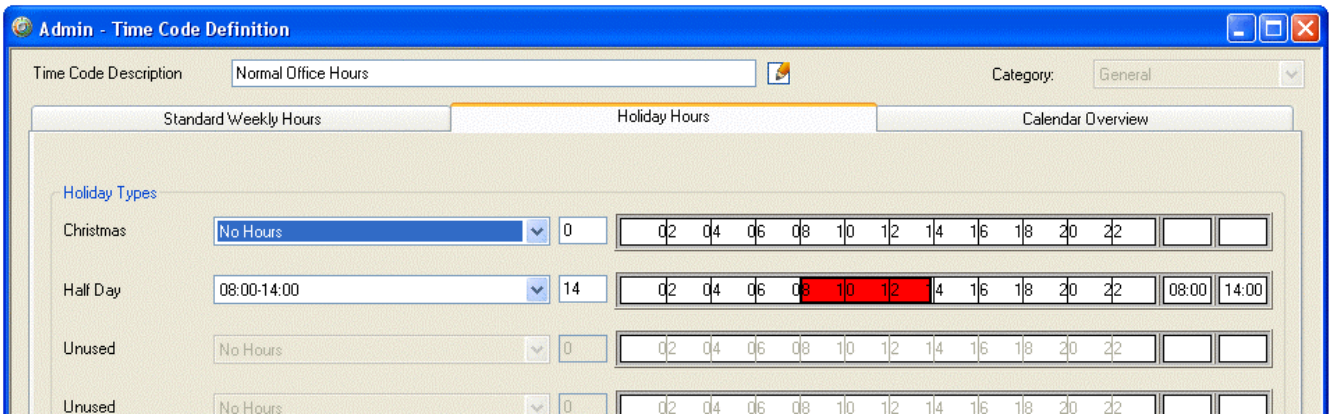
En ayant recours à la fenêtre Configure/System Holiday, on peut introduire les dates de jours fériés, de sorte qu'on puisse déterminer différents temps d'accès pour ces périodes.



Dans la fenêtre System Holiday, on désigne d'abord les types de jour férié dans les boîtes en bas de la fenêtre (p.ex. "Public Holiday" et "Christmas Shutdown"). Ensuite on sélectionne une ou plusieurs dates, puis on clique sur **Assign** et on choisit les types de jour férié pour les attribuer aux dates sélectionnées:



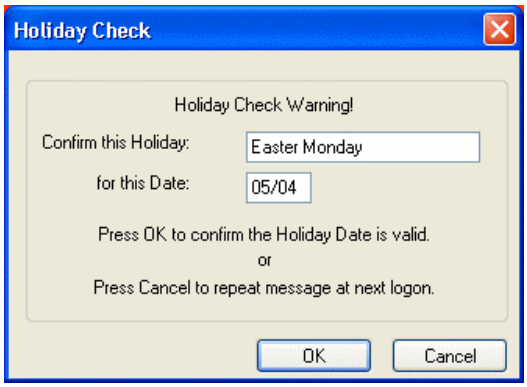
Une fois utilisé la fenêtre de System Holiday pour définir les dates de jour férié, on peut alors aller à l'onglet de Holiday Hours dans la fenêtre Admin/Times/Time Codes pour spécifier les heures correspondantes de chaque type de jour férié. Dans l'exemple suivant pour le code de temps "Normal Office Hours", on voit sélectionné "No Hours" pour le type de jour férié "Christmas Shutdown" et "08:00-14:00" pour la demi-journée "Half Day" comme type de jour férié (p.ex. veille de Noël).



La définition des jours fériés facilite d'ajuster les droits d'accès les jours fériés.

Afficher le dialogue de Holiday Check

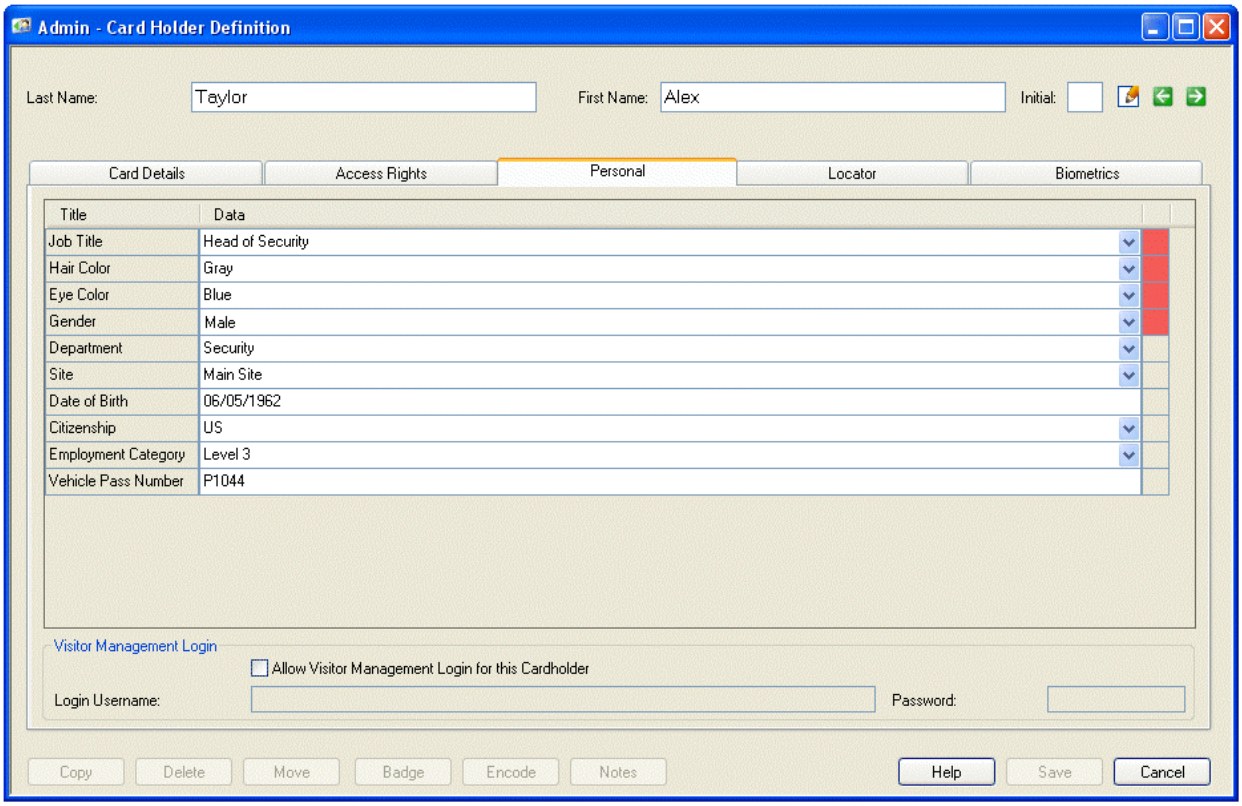
La fenêtre System Holiday Date (date de jours fériés) inclut une option intitulée de **Holiday Check 7 days Prior** (vérifier les jours fériés 7 jours à l'avance). Il est conseillé d'installer cette option, car elle affiche le dialogue de Holiday Check à chaque fois que vous vous connectez pendant les 7 jours précédant un jour férié (de sorte que vous ayez la chance de vérifier que la date de ce jour est correct avant qu'il ne s'approche):



Le dialogue n'est affiché qu'à condition qu'on se connecte au PC-client spécifié de **Route Holiday/Advance/Retard Checks to** dans la fenêtre Configure/Preferences/System (, un dialogue similaire s'affiche pour prévenir le changement des heures d'été/d'hiver).

Spécifier les coordonnées personnelles

On peut utiliser l'onglet Personal de la fenêtre Admin/Card Holder, voir ci-après, pour spécifier les coordonnées personnelles du détenteur de carte.



Les coordonnées personnelles affichées dans cet onglet (p.ex. "Job Title" [emploi], "Hair Color" [couleur des cheveux] et "Gender" [sexe]) figurent dans la fenêtre Admin/Personal/Configure/Card Holder.

Un menu déroulant peut s'afficher pour certains titres de coordonnées personnelles servant à l'information générale comme la couleur des cheveux, le sexe, etc. Pour ces titres on peut sélectionner des données prédéfinies dans les listes du menu déroulant. C'est en fonction de la manière comment les titres ont été installés dans la fenêtre Admin/Personal/Configure/ Card Holder, on a la possibilité de taper le texte directement dans la première case vide de la liste du menu déroulant. Dans ce cas, l'information que vous introduisez s'ajoute automatiquement à la liste et est retenue pour la prochaine fois que vous ouvrez cette fenêtre.

Les titres de coordonnées personnelles qui ne figurent pas dans les listes du menu déroulant servent d'informations qui diffèrent pour chaque personne, p.ex. la date de naissance (Date of Birth). Dans ce cas on tape le texte directement dans la case. S'il y a un masque à remplir dans la fenêtre Admin/Personal/Configure/ Card Holder, il est peut-être nécessaire d'entrer les informations compte tenu d'un format particulier, p.ex. mm/dd/yyyy pour la valeur d'une date.

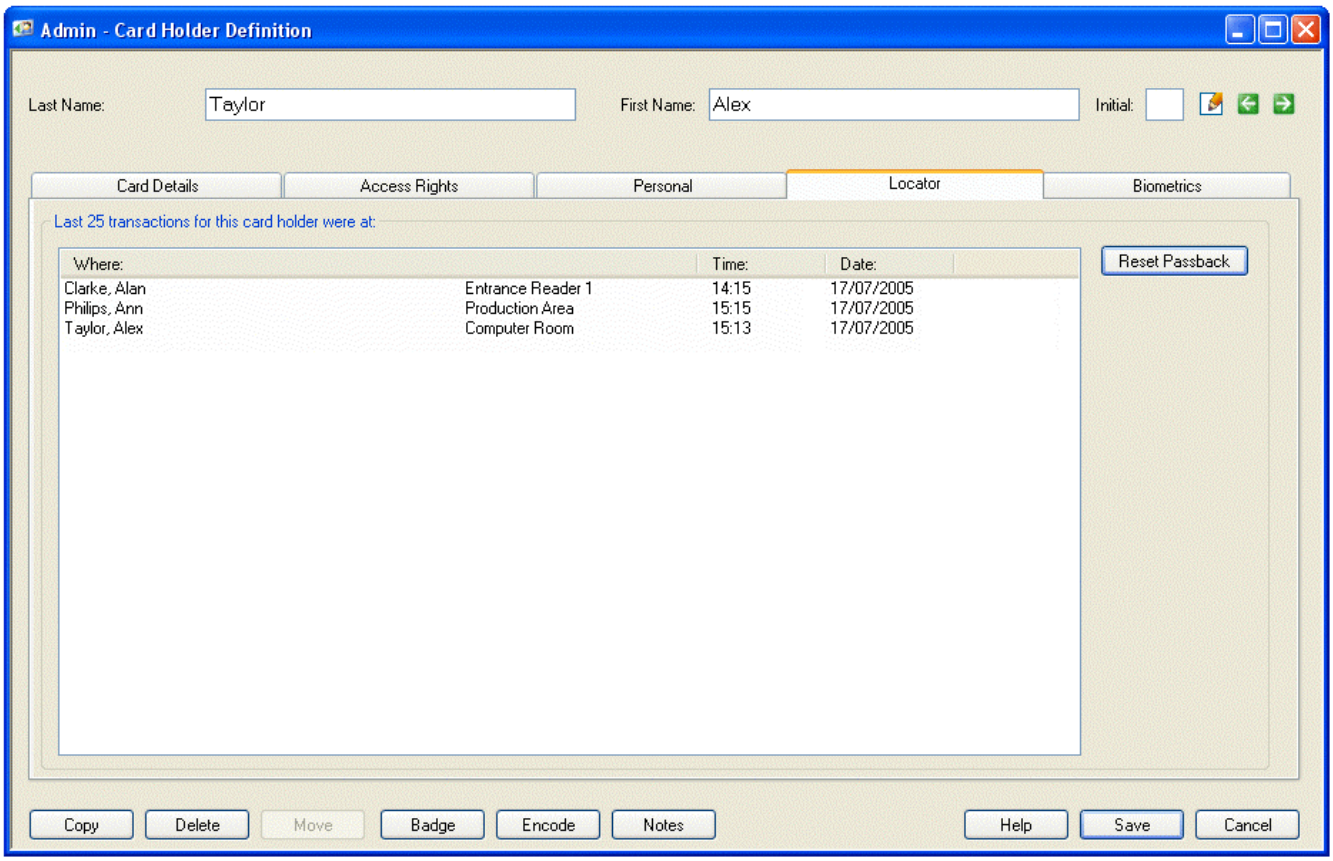
Spécifier les coordonnées personnelles signifie d'avoir des informations supplémentaires utiles concernant le détenteur de carte, ce qui est demandé de temps en temps. Il est en plus possible d'activer les filtres de **Card Data Title** et de **Visitor Data Title** dans la fenêtre Card Holder Selection (la première fenêtre affichée après avoir sélectionné l'option de **Card Holders**). Ces filtres peuvent servir à rechercher le nom d'une personne parmi les coordonnées personnelles spécifiées, p.ex. le numéro d'immatriculation d'un véhicule.

C'est selon les préférences du système, qu'il peut être obligatoire de spécifier les données de quelques uns des titres ou de tout un chacun. Les cases à remplir obligatoirement ont des repères

rouges sur la droite. S'il y a alors ces champs obligatoires, il sera impossible de sauvegarder les éléments du détenteur de carte avant que les coordonnées personnelles spécifiées ne soient entrées.

Localiser un détenteur de carte

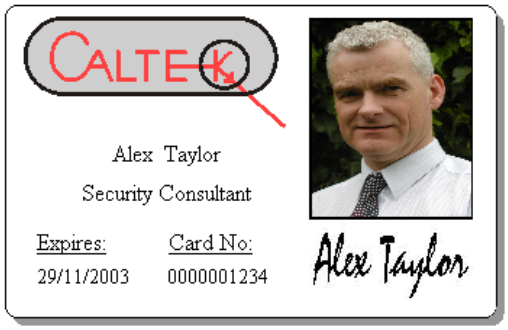
De temps à autre, on veut déterminer le lieu de séjour d'un détenteur de carte dans un bâtiment à un moment donné. Pour le savoir, on peut recourir à l'onglet de localisateur dans la fenêtre de Card Holder, où sont inscrites les 25 dernières transactions faites par le détenteur de carte respective aux lecteurs. Exemple:



Chapitre 4: Produire les badges ID

L'introduction

Le logiciel de gestion de sécurité fournit un grand nombre d'outils qui permettent de concevoir et d'imprimer d'une manière rapide et facile les badges ID. Un badge ne peut être utilisé qu'aux seules fins de l'identification ou du contrôle d'accès, voire même à ces deux fins à la fois.



Produire des badges ID est facile. Il faut d'abord utiliser la fenêtre Tools/Badge Designer pour créer une bibliothèque des badges conçus, ensuite on passe à la fenêtre Admin/Card Holders pour sélectionner, imprimer et encoder un badge pour chaque personne.

La fenêtre Admin/Card Holders permet d'entrer rapidement toutes les informations nécessaires à concevoir le badge, telles que le nom du détenteur de carte et le numéro du badge. On peut également prendre la photo de la personne, sa signature et toutes les données biométriques, ensuite on imprime et encode la carte, tout cela se fait à partir de la même fenêtre. L'interface utilisateur a été conçue pour optimaliser l'efficience de l'opération, pendant qu'un contrôle général est possible, y compris toutes les visualisations graphiques et informations requises, personnalisées à vos propres besoins.

Ce chapitre décrit plus en détail le processus de production des badges. Pour se familiariser avec le processus on peut interroger en interaction le programme éducatif que l'on appelle via le menu d'aide (Help) du logiciel SMS.

Concevoir les badges

On peut concevoir des badges à l'aide de la fenêtre Tools/Badge Designer. La conception du badge définit l'apparence du badge, y compris l'emplacement et la nature des informations à y mettre. Le modèle d'un badge pourrait p.ex. contenir le nom du détenteur de carte, la date d'expiration, le logo de la société et la photo du détenteur de carte. Le système offre tous les outils nécessaires à créer en quelques minutes le badge adapté aux besoins de l'utilisateur, y compris le texte et les graphiques à y appliquer des deux côtés du badge.

En se servant du designer de badges, on peut créer une bibliothèque de modèles de badges. On peut p.ex. décider de créer différents formats pour le personnel d'adminisatration, de nettoyage, les sous-traitants et l'équipe de sûreté.

Une fonction principale du designer de badges consiste dans la possibilité d'associer les droits d'accès standard à chaque format de badge destiné aux fins du contrôle d'accès. Chaque détenteur de carte auquel est attribué ce modèle de badge bénéficie automatiquement des droits d'accès liés à ce format de badge, de sorte qu'il devienne inutile d'attribuer individuellement les droits d'accès pour chaque personne.

La simplicité du logiciel, au surplus l'aide rapportée au contexte et un programme éducatif interactif, assurent que tous ceux ayant des connaissances de base en maniement d'une souris et d'un clavier peuvent commencer à travailler rapidement et efficacement avec le designer de badge.

La figure 4.1 donne un aperçu des éléments principaux offerts par le Badge Designer.

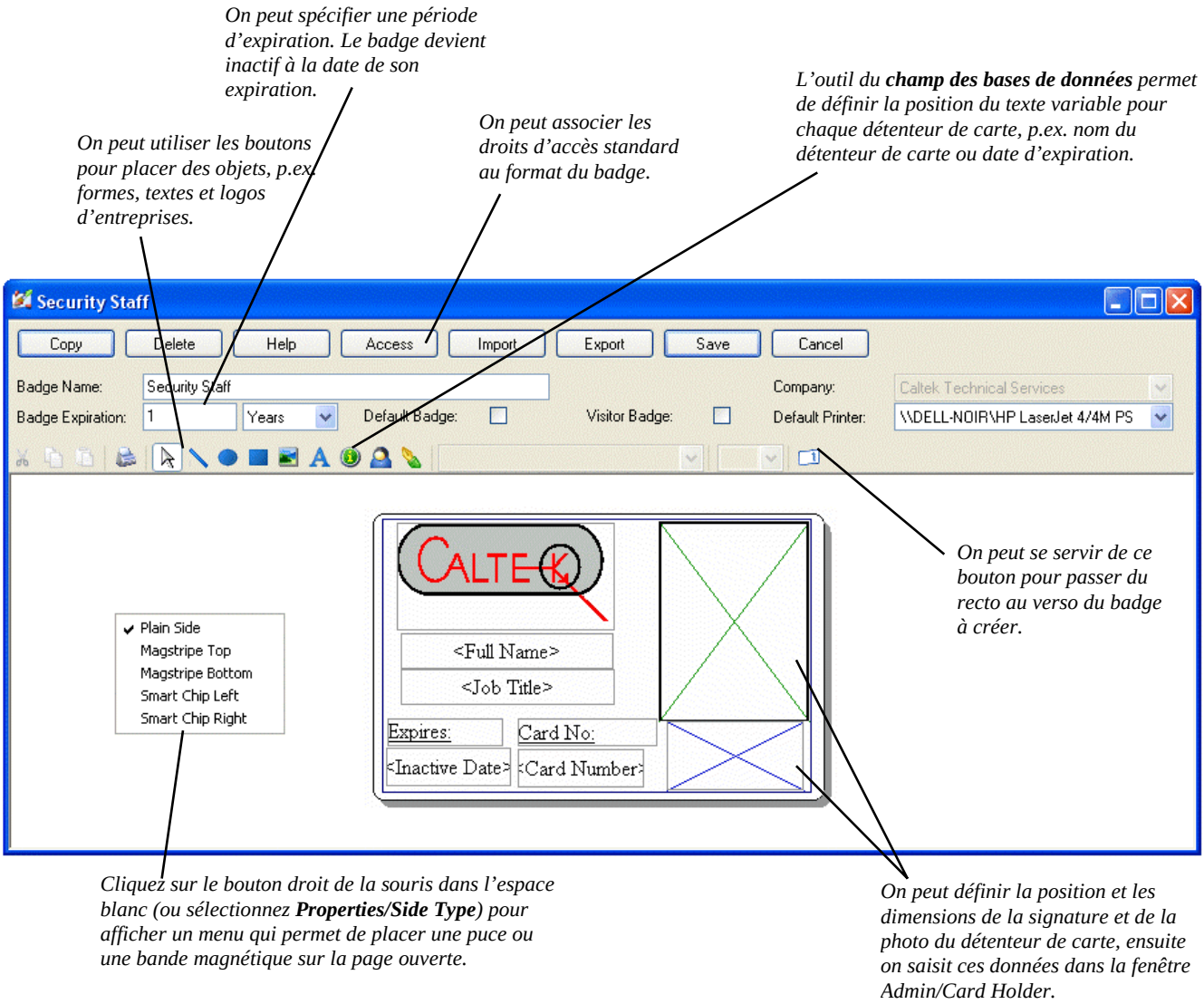

On peut spécifier une période d'expiration. Le badge devient inactif à la date de son expiration.
On peut utiliser les boutons pour placer des objets, p.ex. formes, textes et logos d'entreprises.
On peut associer les droits d'accès standard au format du badge.
L'outil du champ des bases de données permet de définir la position du texte variable pour chaque détenteur de carte, p.ex. nom du détenteur de carte ou date d'expiration.
Security Staff
Copy
Delete
Help
Access
Import
Export
Save
Cancel
Badge Name:
Security Staff
Badge Expiration:
1
Years
Default Badge:
Visitor Badge:
Company:
Caltek Technical Services
Default Printer:
\\DELL-NOIR\HP LaserJet 4/4M PS
Plain Side
Magstripe Top
Magstripe Bottom
Smart Chip Left
Smart Chip Right
<Full Name>
<Job Title>
Expires:
Card No:
<Inactive Date>
<Card Number>
On peut se servir de ce bouton pour passer du recto au verso du badge à créer.
Cliquez sur le bouton droit de la souris dans l'espace blanc (ou sélectionnez Properties/Side Type) pour afficher un menu qui permet de placer une puce ou une bande magnétique sur la page ouverte.
On peut définir la position et les dimensions de la signature et de la photo du détenteur de carte, ensuite on saisit ces données dans la fenêtre Admin/Card Holder.

Figure 4.1: La fenêtre de Badge Designer Definition

Dans la fenêtre Badge Designer la barre de menu change pour inclure des options nécessaires à la création de badges.

Produire un badge de détenteur de carte

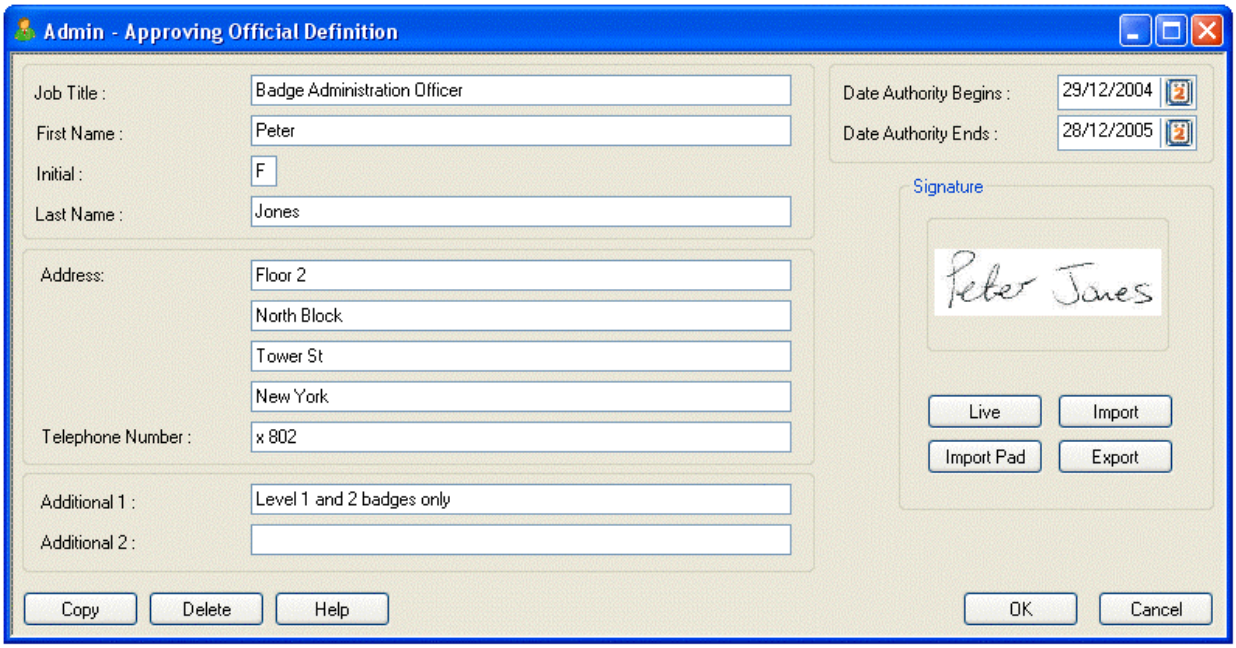
Après avoir fait les modèles de badge, on peut sélectionner le badge de chaque détenteur de carte dans la fenêtre Admin/Card Holders, comme décrit ci-après.

Entrer les éléments de carte et prendre la photo du détenteur de carte

D'abord il faut vérifier que les coordonnées du détenteur de carte sont correctes et que sa photo a été prise (en supposant qu'une photo soit à imprimer sur le badge). A cette fin on utilise l'onglet Card Details, comme décrit à la page **Error! Bookmark not defined.**.

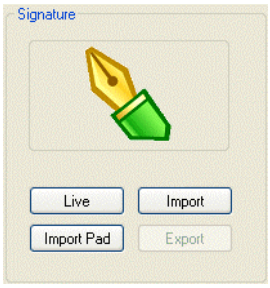
Approbation de la personne autorisée

L'onglet Card Details comprend une option **Approving Official** qui sert à choisir le nom de la personne étant autorisée à recevoir le badge. On peut installer l'approbation des personnes autorisées dans la fenêtre Admin/Approving Official:



Saisir la signature du détenteur de carte

S'il s'agit d'imprimer la signature du détenteur de carte sur le badge, elle est à mettre sur l'emplacement prévu à cette fin:



Il y a trois possibilités de saisir une signature:

- **Live** – On clique sur ce bouton pour saisir la signature prise directement par une caméra connectée au PC.
- **Import** – On clique sur ce bouton pour importer une signature stockée (p.ex. reprise par une caméra numérique).
- **Import Pad** – On clique sur ce bouton pour saisir en ligne la signature depuis un tapis de signature attaché à l'ordinateur. Le détenteur de carte écrit sa signature sur ce support, et le système la saisit automatiquement.

Une fois la signature est saisie, l'icône démontrée ci-dessus est remplacée par la signature réelle de la personne.

Saisir l'empreinte digitale et les données biométriques de la main

La reconnaissance biométrique est devenue de plus en plus importante comme une solution à répondre à la nécessité de nos jours toujours croissante visant à assurer la sécurité totale. Le logiciel de gestion de sécurité s'appuie sur les technologies les plus récentes pour permettre la géométrie d'empreinte digitale et de la main mise en œuvre comme une part des transactions du contrôle d'accès.

Les donnés d'empreintes digitales et de géométrie biométrique de la main peuvent être saisies dans l'onglet Biometrics, ce qui facilite d'introduire les éléments du détenteur de carte, de saisir les données biométriques et de produire un badge depuis un seul lieu dans l'interface utilisateur.

Après avoir saisi les données biométriques, on peut se servir du module optionnel de gestion des cartes à mémoire pour encoder les données biométriques sur une carte à mémoire, que le détenteur de carte présente à un lecteur biométrique pour avoir l'accès. Le lecteur contrôle les données de la main ou de l'empreinte digitale sur la carte et les comparent à la main présentée ou à l'empreinte digitale réelle pour confirmer l'identité de la personne respective.

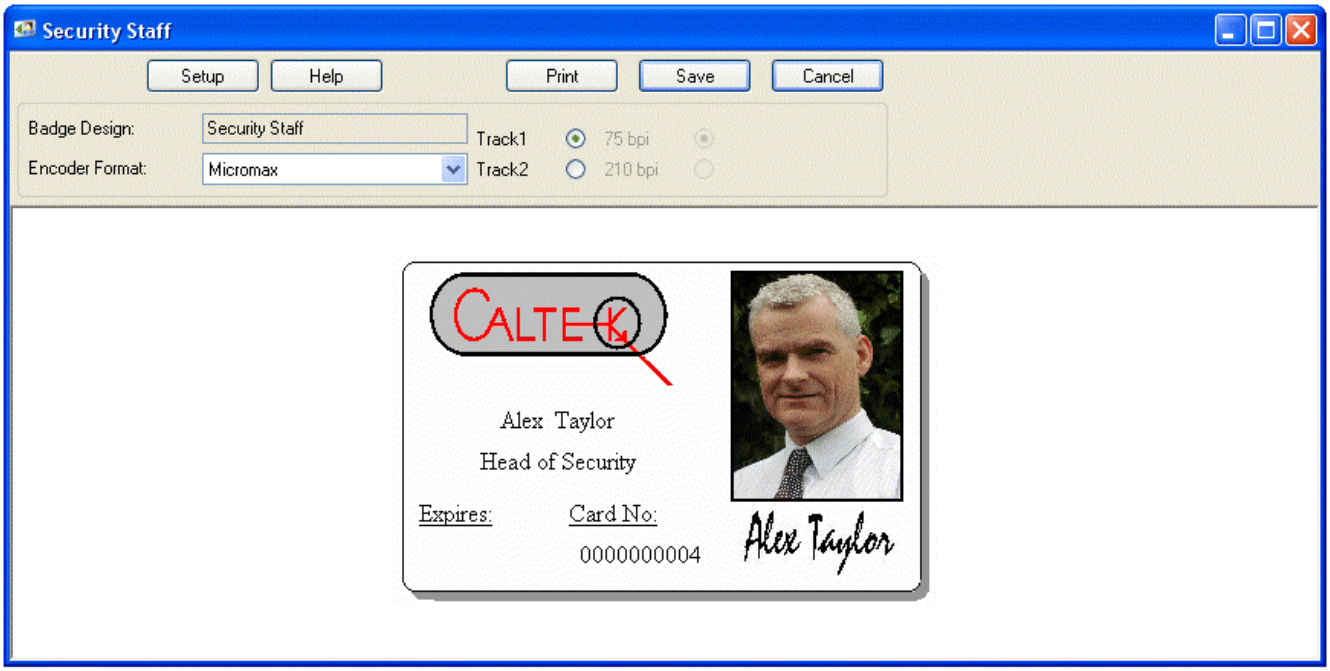
La technologie des cartes à mémoire permet d'utiliser une carte individuelle multifonction.

Pour des informations plus détaillées, se référer au programme d'aide de logiciel SMS. Alternativement, si l'on utilise les lecteurs d'empreinte digitale 813, le manuel *813 Fingerprint Reader User's Guide* fournit d'autres détails concernant l'inscription des empreintes digitales et l'utilisation des lecteurs du type 813.

Sélectionner et présenter la conception du badge

Avant d'imprimer un badge, il faut choisir une conception de badge pour le détenteur de carte au menu déroulant de **Badge Design** dans l'onglet Card Details.

Une fois le modèle du badge sélectionné, on peut actionner le bouton **Badge** en bas de la fenêtre Card Holders pour voir la présentation du badge. Le nom du détenteur de carte, sa photo, etc. sont automatiquement insérés à l'emplacement approprié. Ci-après un exemple du badge tel qu'il est proposé à la page 4-2.



Dans la fenêtre Preview est inluse une option du format d'encodage (**Encoder Format**). Si votre imprimante de badges dispose d'un encodeur à bande magnétique incorporée, elle peut encoder le numéro de carte, le code client et le numéro d'émission sur la bande magnétique. Pour profiter de cette facilité, il suffit de choisir le format d'encodage (**Encoder Format**) dans le menu.

Imprimer le badge

Si l'on veut imprimer un badge individuel, on procède simplement à sélectionner **Print**, pendant qu'on regarde le format définitif du badge dans la fenêtre de Card Holder, tel qu'il est présenté dans la figure précédente. Une imprimante convenablement combinée avec un encodeur devrait sortir la carte imprimée et encodée en une seule opération.

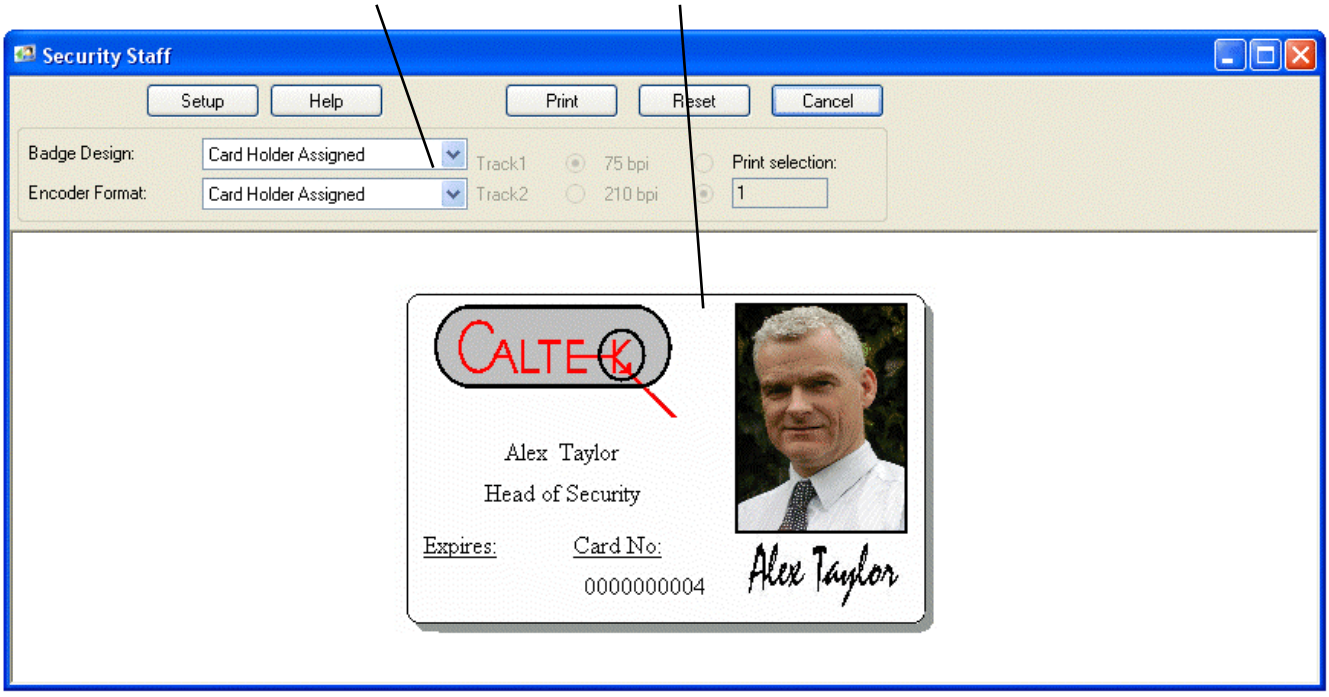
Alternativement on peut sauvegarder les coordonnées du détenteur de carte et imprimer en une et même opération plusieurs badges à l'aide de la fenêtre Admin/Print Badges.

Lorsqu'on se décide pour la fenêtre Admin/Print Badges, la sélection des formats de badge et d'encodage choisis dans la fenêtre Card Holder sont traités comme prescrits, ce qu'on peut négliger par la fenêtre Print Badges.

Comme c'est le cas pour la plupart des options du menu d'administration, une fenêtre de sélection s'affiche par Admin/Print Badges, où l'on peut sélectionner les badges à imprimer. Ceci fait, la fenêtre Print Badges apparaît, telle que présentée dans la figure ci-après. En cliquant sur **Print** on débute la procédure d'impression/d'encodage.

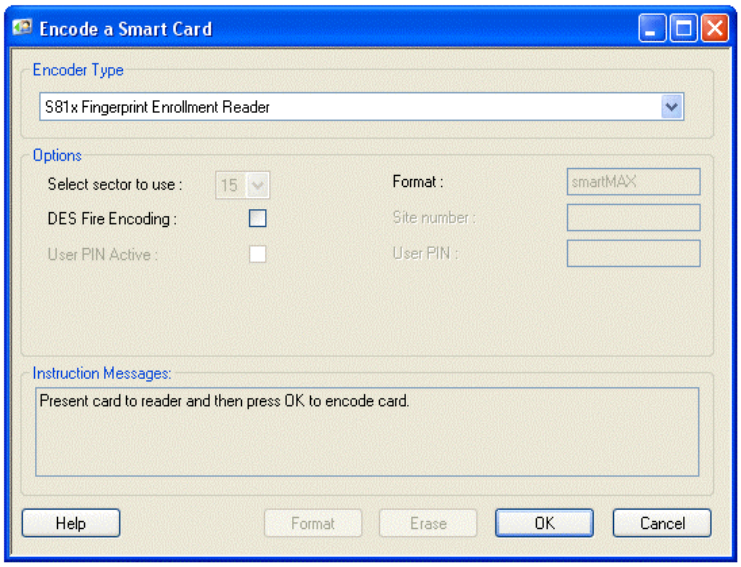
On peut remplacer le format standard de badge et d'encodage pour chaque détenteur de carte.

Le badge de chaque personne est affiché tel qu'il est imprimé.



Encoder le badge (la carte)

Si l'option de coût de "Smart Card Encoding" est installée, on peut actionner un bouton **Encode** dans la fenêtre Card Holder. en cliquant sur **Encode** la fenêtre ci-dessous s'ouvre, qui permet d'encoder le numéro de carte et les données biométriques optionnelles sur le badge, s'il s'agit d'une carte à mémoire telle qu'elle est utilisée aux fins du contrôle d'accès:

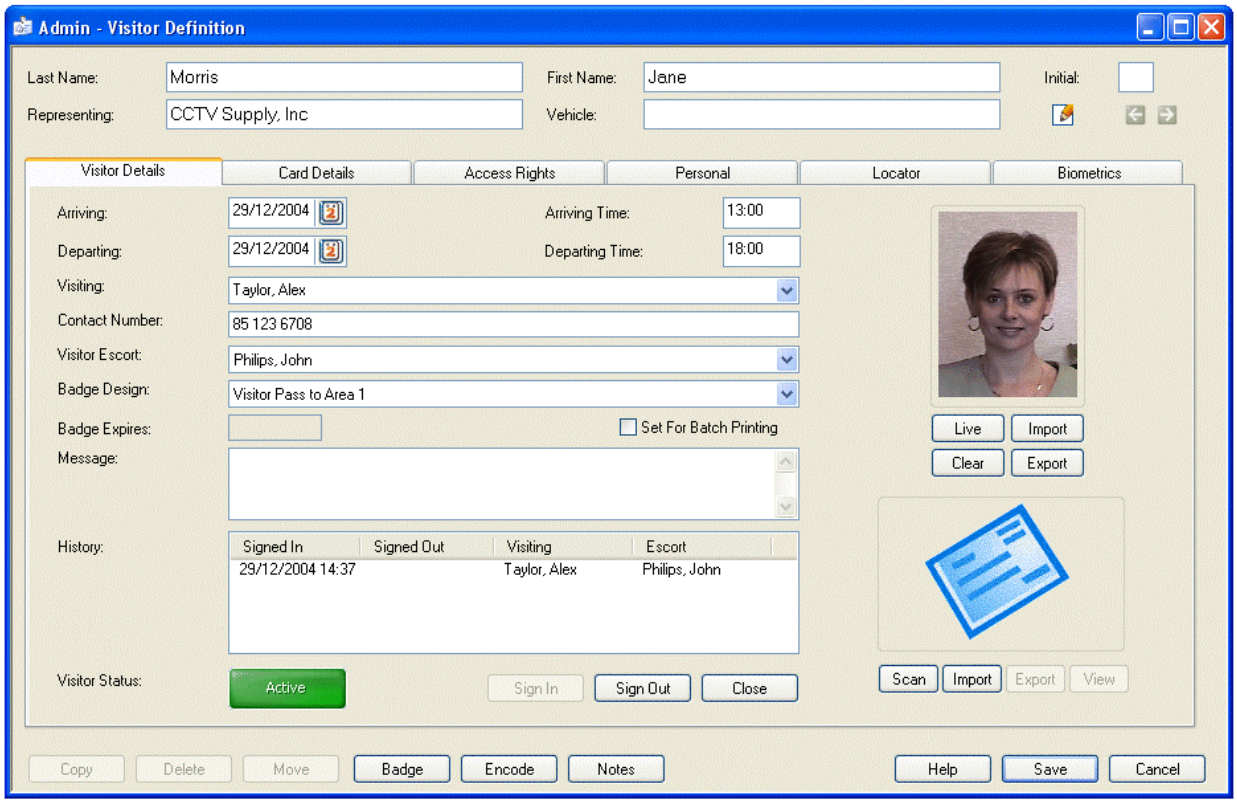


Le logiciel SMS traite des types de cartes à mémoire très variés, y compris les suivants: Philips® MIFARE®, Philips MIFARE DESfire, HID®, HID i*CLASS*™ et Texas Instruments™ (ISO 15693). Ce logiciel s'approprie également à l'emploi de quelques encodeurs offerts par différents fabricants.

Chapitre 5: La gestion des visiteurs

La création des visiteurs

Les fonctions de la gestion des visiteurs du logiciel de gestion de sécurité permettent d'améliorer l'efficacité de la procédure du contrôle des visiteurs, d'augmenter la sécurité sur les lieux et de mettre à jour plus rationnellement les coordonnées des visiteurs. Le système permet l'entrée facile des éléments détaillés des visiteurs à l'aide de la fenêtre spécialement prévue à cette fin Admin/Visitor et accessible depuis chaque PC-client ou navigateur Web (par l'option d'accès au Web):



La fenêtre peut être utilisée par tout employé autorisé à entrer des informations personnelles concernant les visiteurs avant qu'ils n'arrivent sur place. Cette procédure peut sensiblement réduire les retards du contrôle d'accès, améliorer son efficacité et mettre le personnel de sécurité en mesure de vérifier avec plus de soins l'identité d'une personne à son arrivée.

La fenêtre Admin/Visitor a été conçue d'une manière à éviter que des gens qui ne sont normalement pas d'utilisateurs du logiciel de gestion de sécurité entrent des éléments personnels des visiteurs. La fenêtre Visitor ressemble à l'onglet de personnel de la fenêtre Admin/Card Holder.

Il est possible de donner à divers usagers des niveaux différents d'accès à la fenêtre Admin/Visitors. Il se peut que certains onglets dans la fenêtre ne sont pas actifs, ce qui dépend des options consenties à l'usager (comme elles sont définies dans la fenêtre Configure/User/Profiles).

Les coordonnées des visiteurs

L'onglet Visitor Details permet de spécifier les éléments généraux du visiteur, p.ex. quand on attend que le visiteur arrive et repart, à qui il/elle veut rendre visite tout comme le nom de celui qui lui fait escorte (si besoin est). C'est de la même manière que pour la fenêtre Admin/Card Holders, que l'on peut prendre la photo du visiteur, choisir le modèle du badge, imprimer ensuite le badge du visiteur sur une imprimante correspondante.

Un avantage important du module de SMS Visitor Management consiste dans la possibilité d'enregistrer les visiteurs dans l'onglet Visitor Details à leur arrivée et à leur départ, grâce aux boutons **Sign In** et **Sign Out**. Tous les éléments de l'arrivée et du départ du visiteur sont sauvegardés dans la boîte History se trouvant en bas de la fenêtre.

L'état du visiteur à un moment donnée (Pending, Active ou Closed) est affiché dans une boîte à identifier par la couleur du côté gauche au coin en bas de la fenêtre, qui permet de visualiser immédiatement si le visiteur se trouve encore sur le site.

Il y a un autre avantage, c'est la possibilité d'afficher une photo du visiteur lue par un scanneur ou importée depuis sa carte de visite dans l'onglet Visitor Details. Cette caractéristique économisant du temps assure l'acquisition rapide et précise d'informations de base sur le visiteur, p.ex. l'adresse et les coordonnées de contact, ce qui est particulièrement utile dans le cas où les éléments du visiteur n'ont pas été introduits avant son arrivée.

Les coordonnées personnelles

La fenêtre Admin/Visitors comprend un onglet Personal, où on peut introduire les coordonnées personnelles du visiteur d'une même manière que pour l'onglet Personal de la fenêtre Admin/Card Holders (Cf. page **Error! Bookmark not defined.**).

Les titres des coordonnées personnelles (p.ex. "Visitor's Company Name" [raison sociale de la sté du visiteur], "Reason for Visit" [motif de la visite], "Visit Arranged By" [visite arrangée par], "Hair Color" [couleur des cheveux], etc.) diffèrent de ceux utilisés pour les détenteurs de carte et sont installés dans la fenêtre Admin/Personal/Configure/Visitor.

Les titres prédéfinis des éléments de chacun de ces titres de coordonnées personnelles peuvent être indiqués dans la fenêtre Admin/Personal/Visitor Data. Exemple: Pour la couleur des cheveux on peut définir les titres comme "Black", "Brown" et "Blonde". Les titres prédéfinis peuvent être sélectionnés parmi les éléments proposés dans le menu de la fenêtre.

Les détails de carte de visiteur, les droits d'accès et la biométrie

Si le visiteur a besoin d'une carte à présenter au contrôle d'accès, il faut spécifier un numéro de carte et d'autres éléments dans l'onglet Card Details. Il faut également recourir à l'onglet Access Rights pour déterminer à quelles zones le détenteur de carte peut accéder et à quelles heures. Installer les éléments de carte et les droits d'accès d'un visiteur signifie à peu près la même procédure que pour

l'introduction des éléments de carte et des droits d'accès d'un détenteur de carte standard, telle qu'elle est décrite à la page 3-4 et **Error! Bookmark not defined.**.

S'il existe des lecteurs de cartes biométriques, il peut être nécessaire de saisir les empreintes digitales du visiteur ou la géométrie de sa main avant d'encoder la carte du visiteur pour le contrôle d'accès. A cette fin on utilise l'onglet Biometrics, de la même manière que pour un détenteur de carte standard (Cf. page **Error! Bookmark not defined.**). Si les cartes à bande magnétique sont d'usage, on peut encoder la carte au même moment qu'elle est imprimée (à condition que l'on utilise un appareil combiné d'imprimante de badge et d'encodeur).

Une fois le visiteur a quitté le site, il est possible d'effacer le numéro de carte parmi les coordonnées du visiteur enregistrées dans la fenêtre Admin/Card Holder, ensuite on sauvegarde les éléments. C'est ainsi qu'on peut redistribuer le numéro de carte à un autre visiteur sans effacer les données enregistrées du visiteur précédent, auxquelles on peut avoir recours lorsqu'il revient sur le site.

Les rapports de visiteurs

Le système offre un bon nombre de possibilités pour établir des rapports relatifs aux visiteurs:

- **Admin/Reports/Visitors** – On peut lister les détails des cartes de visiteurs.
- **Admin/Reports/Access** – On peut lister les détails des droits d'accès des cartes de visiteurs.
- **View/History/Activity** – On peut visualiser les alarmes et événements déclenchés précédemment par des visiteurs.
- **View/History/Card Holders Onsite** – On peut retrouver lesquels des visiteurs sont passés par un lecteur d'entrée.
- **View/Locator** – On peut localiser certains visiteurs sélectionnés à un moment voulu.
- **View/Muster** – La liste de présence (roll call) incluent les visiteurs.

Toutes les transactions de visiteurs aux portes du contrôle d'accès sont enregistrées, et toute infraction à la sécurité du site est immédiatement transmise.

Chapitre 6: La gestion de vidéo numérique

Introduction

Le module optionnel de la gestion de vidéo numérique permet d'intégrer les systèmes CCTV et enregistrement vidéo numérique. Le module permet de visionner et d'enregistrer les images des caméras de surveillance à partir d'écrans qui sont intégrés au système SMS et sont faciles à utilisés.

Deux versions du module sont disponible: la version "Essentiels Vidéo" et la version complète. Le tableau 1 de la page suivante donne un aperçu des caractéristiques des deux produits.

Le module de gestion vidéo numérique offre une plateforme ouverte supportant les caméras IP[1] connectées directement au réseau G4Tec Edge-of-Network Video Servers (ENVS) et à une large gamme d'enregistreurs numériques (DVR), comme documenté dans le *Guide d'installation du logiciel*.

Un ENVS ou un DVR (Magnétoscope numérique) est un appareil qui peut enregistrer et stocker des images à partir de toutes les caméras connectées. Les images peuvent, si nécessaire, enregistrées de façon continue ou à des heures définies du jour et de la nuit. L'enregistrement local sur un système ENVS ou un DVR évite d'avoir à transmettre la vidéo à travers le réseau pour l'enregistrement et contribue ainsi à la réduction du trafic réseau.

L'ENVS offre une solution extrêmement économique pour les organisations qui ont besoin d'enregistrer, de stocker et de visionner les vidéos prises en temps réel. Chaque système ENVS peut simultanément contrôler et enregistrer des vidéos à partir de quatre cameras et des unités multiples peuvent être aisément connectées à n'importe quelle place dans le réseau pour offrir un soutien de proximité aux unités qu'elles contrôlent.

Ce chapitre donne un aperçu des écrans et options disponibles dans le module de gestion de vidéo numérique.

Note: L'enregistrement de vidéos à partir de cameras IP est disponible uniquement si l'option "Logiciel du serveur de sauvegarde vidéo " est aussi installée (page **Error! Bookmark not defined.**).

[1] IP cameras are available only with the full Digital Video Management Module.

Tableau 1: Comparaison des caractéristiques entre les modules "Essentiels vidéo" et "Gestion vidéo numérique complet"

	Différences entre les types de produits	
Caractéristiques	**Logiciel essential vidéo**	**Module gestion vidéo numérique complet**
Écran matrice virtuelle – Affiche simultanément de multiples images en temps réel à partir des caméras vidéo numériques. Inclus les contrôles pour le panoramique, l'élévation, le zoom et la mise au point caméra. Dispositif d'enregistrement instantané	Un maximum de 4 images en temps réel.	Un maximum de 36 images en temps réel Séquençage caméra. Support l'affichage de pages Web. Dispositif de visionnage instantané Affichage alarme et activité.
Écran de visionnage vidéo – Permet le visionnage aisé des enregistrements vidéo. Des options de filtrage permettent aux enregistrements d'être retrouvés facilement dans la base de donnée.	Visionnage d'un enregistrement unique.	Visionnage simultané d'un maximum de 4 enregistrements. Possibilité de marquer les zones d'intérêts. Export d'images JPEG
Écran de vérification vidéo[2] - Permet à un opérateur de comparer l'image vidéo, d'un détenteur de cartes, prise en temps réel à l'image enregistrée de la personne.		
Support caméra – Supporte les caméras reliées au système ENVS (Edge-of-Network Video Servers) et d'enregistrement numérique DVR.. Le nombre maximum de caméra dépend de la licence. Le maximum système est de 64.		Support des caméras IP.
Intégration connecteur caméras vidéo – Les caméras reliées à des connecteurs de caméras vidéo peuvent être contrôlés et connectés à chaque moniteur..		
Commandes – Les commandes peuvent, par exemple, exécuter des enregistrements programmés et enregistrer automatiquement les incidents.		Supporte les commandes pour connecter les vidéos en temps réel à la matrice virtuelle.
Visionnage des rapports et des alarmes – Les incidents enregistrés automatiquement peuvent être aisément visionnés à partir de l'écran Affichage/Alarmes ou des rapports historique		
Intégration graphique – La vidéo en temps réel peut être visionnée à partir d'un graphique comme par exemple le plan d'un bâtiment.		

[2] La vérification vidéo est disponible en standard avec le logiciel SMS de gestion de la sécurité, mais les caméras vidéo numériques peuvent être utilisées si le logiciel de gestion vidéo numérique est installé.

Utiliser l'écran de matrice virtuel

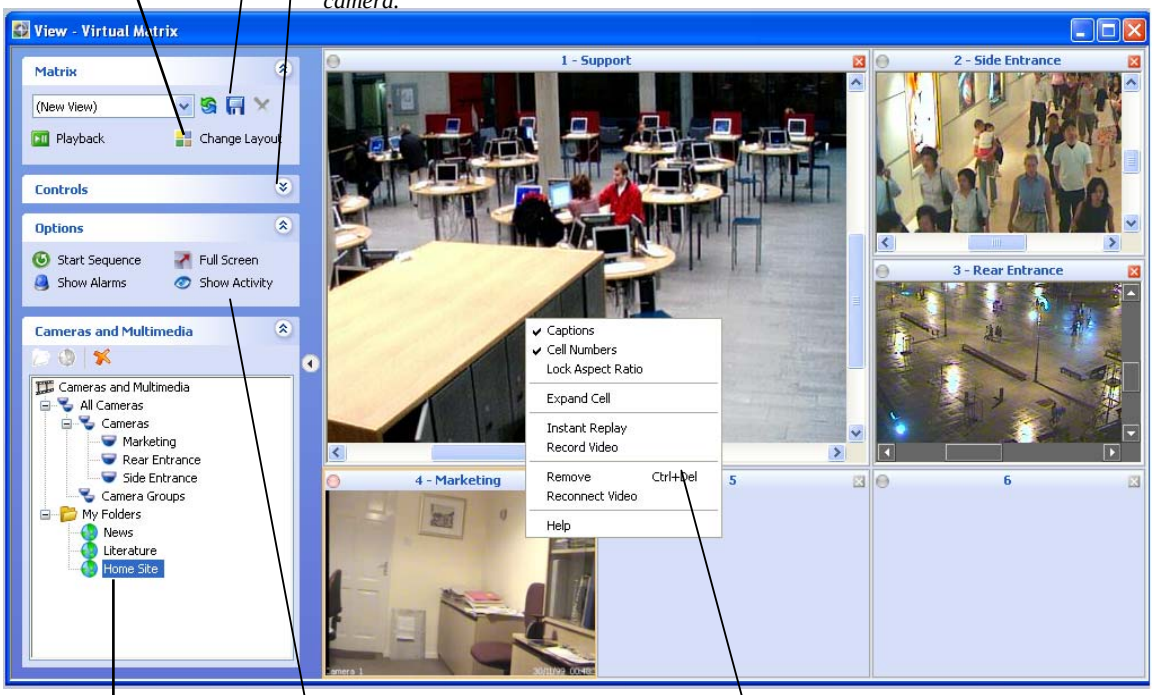
L'écran de matrice virtuelle Affichage/Vidéo numérique/Matrice virtuelle vous permet de visionner simultanément des images en direct à partir d'un maximum de 36 caméras ou pages Web. Chaque image est affichée dans une "cellule" située du côté droit de l'écran.

Pour afficher des images en direct, il faut sélectionner la caméra dans l'arborescence, puis la déplacer et la poser dans une cellule. Vous pouvez aussi déplacer des images de la même façon d'une cellule à une autre. Un double clic sur une image affiche l'image dans la cellule la plus grande.

*Vous pouvez modifier le nombre de cellules affichées et leurs positions en utilisant l'option **Modification de la présentation.***

*Une fois que vous avez décidé des caméras et/ou pages Web à afficher, et que vous avez placé ces objets dans une cellule, vous pouvez sauvegarder la configuration comme un "affichage" en utilisant le bouton **Enregistrer**. La fois suivante où vous ouvrez l'écran, vous pouvez sélectionner l'affichage à partir du menu déroulant, qui affiche automatiquement les pages Webs ou les images des caméras dans cet affichage.*

Un clic á cet endroit peut afficher un contrôle pour effectuer un zoom avant/arrière, un panoramique, une modification de l'élévation et faire la mise au point de la caméra. Le contrôle ne permet l'accès qu'aux fonctions qui sont supportées par la caméra.



*L'arborescence contient les paramètres des caméras vidéos numériques dans les écrans d'installation et toutes les pages Web[1] ajoutées en utilisant le bouton **Créer URL** qui est placé au dessus de l'arborescence.*

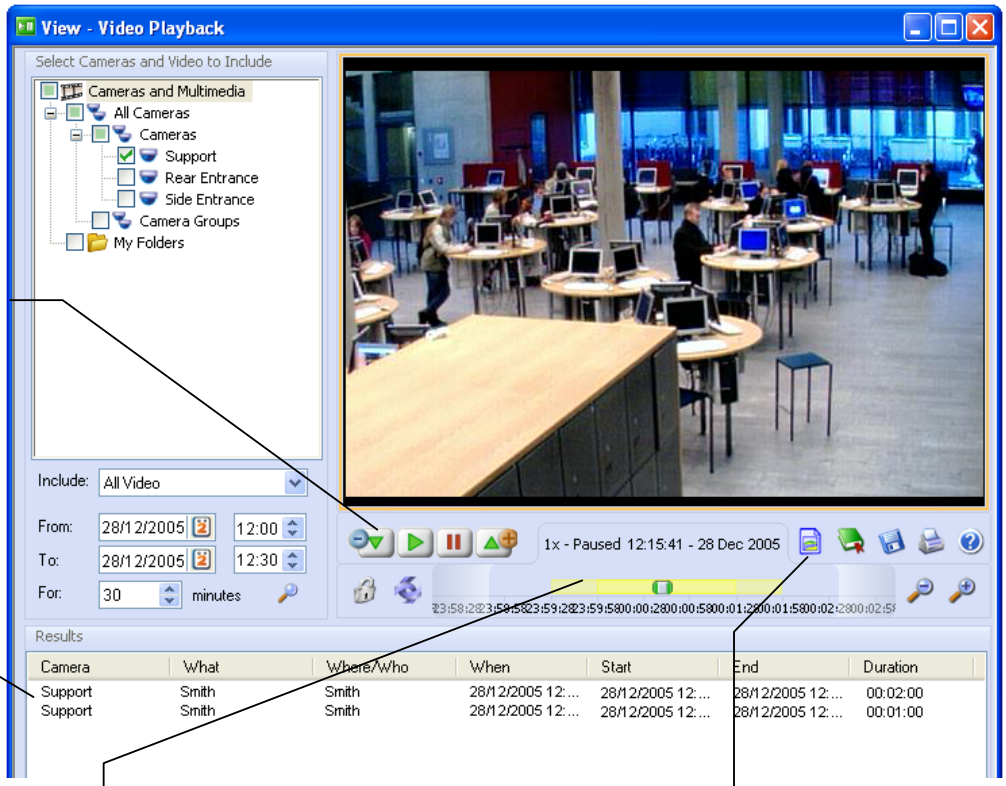
Ce panneau est disponible lorsque la version complète du logiciel est utilisée. Vous pouvez démarrer le séquençage vidéo, afficher une image en plein écran, lister des alarmes et afficher l'activité actuelle.

Le menu clic-droit propose des options contextuelles; par exemple pour enregistrer des vidéos ou visionner les dernières 5 minutes de vidéo..

Utiliser l'écran de visionnage vidéo

L'écran de visionnage vidéo Affichage/Vidéo numérique/Visionnage vidéo vous permet de visionner simultanément jusqu'a quatre enregistrements de caméra vidéo numériques. Chaque image est affichée dans une "cellule" placée sur le côté droit de l'écran. Vous pouvez changer entre l'affichage d'une ou de quatre cellules en effectuant un clic droit sur une cellule et en sélectionnant/désélectionnant **Agrandir la cellule (Expand Cell).**

Vous pouvez changer la vitesse de visionnage ou faire une pause ou visionner l'enregistrement.



Ceci liste les enregistrements disponibles pour les caméras sélectionnées.

La barre de défilement affiche les périodes pendant lesquelles les enregistrements existent pour la cellule actuellement sélectionnée. Vous pouvez effectuer un déplacer-lacher du marqueur pour effectuer le visionnage à partir d'un moment différent. Les couleurs différentes de la barre de défilement indiquent différent types d'enregistrement comme les enregistrements marqués[1] ou des enregistrements démarrés par une condition d'alarme.

Vous pouvez utiliser ces options pour effectuer des actions telles que la sauvegarde des enregistrements sous le format AVI, effectuer un zoom avant ou arrière de la barre de défilement et marquer[1] les zones d'intérêts.

Pour visionner un enregistrement:

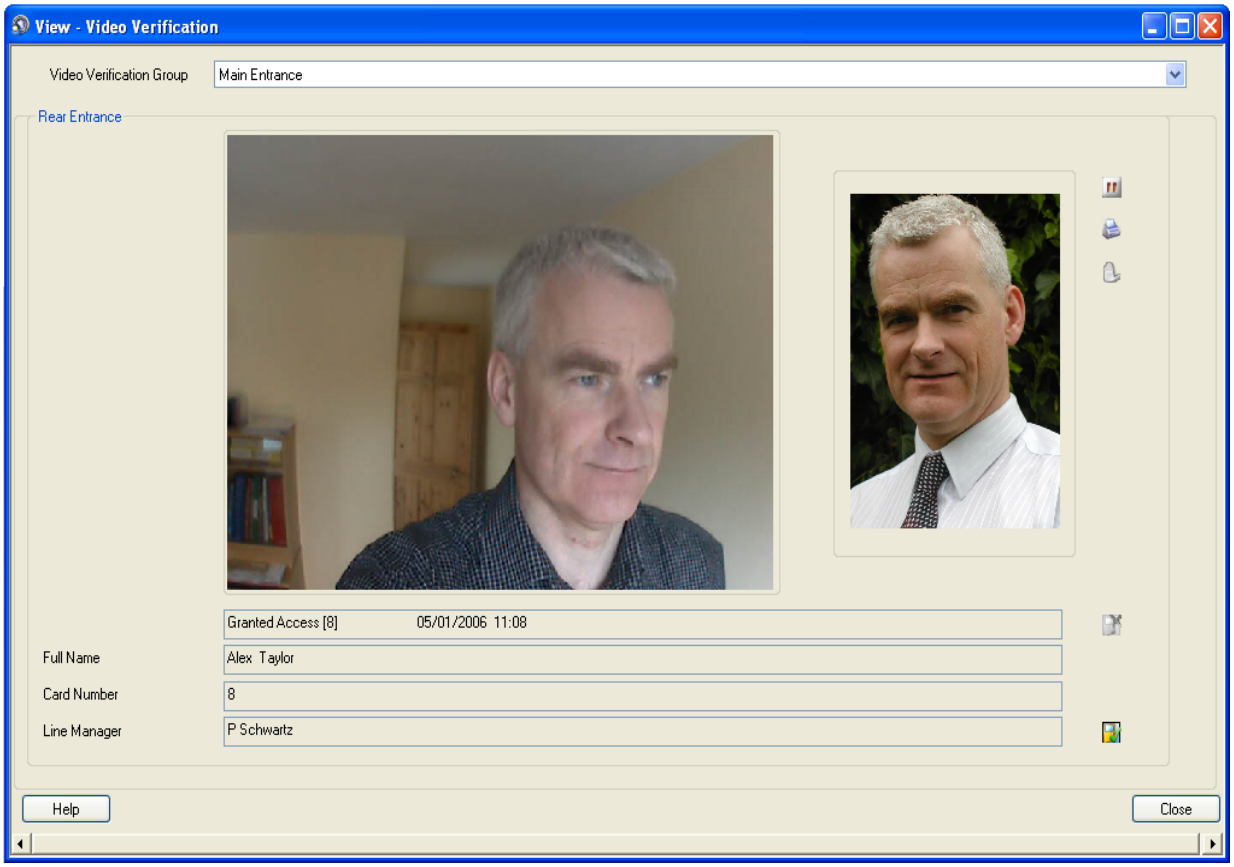
1. Sélectionner la caméra dans l'arborescence située du coté supérieur gauche de l'écran puis sélectionner la caméra qui a été utilisée pour l'enregistrement.
2. Utiliser le menu déroulant **Inclure** pour spécifier les types de vidéo que vous recherchez dans la banque de donnée. Sélectionner ensuite **Toutes les vidéos par horaire** si vous désirez trouver tous les enregistrements.
3. Utiliser le panneau relatif aux dates et horaires pour spécifier la date et la plage horaire des enregistrements à trouver.
4. Cliquer sur le bouton **Chercher.** Le panneau des résultats liste tous les enregistrements qui répondent aux critères et incluent toutes les parties de la période horaire spécifiée par les champs **À partir de** et **Jusqu'à**.

5. Déplacer et poser tous les enregistrement listés dans le panneau des résultats dans une cellule ou double-cliquer. Le visionnage démarre à partir du démarrage de l'enregistrement sélectionné.

Utiliser la vérification vidéo

L'écran de vérification vidéo Affichage/Vérification vidéo affiche des vidéos en temps réel à partir de toutes les caméras dans un groupe de vérification vidéo sélectionné, comme défini dans l'écran Administration/Groupe/Vérification vidéo. Un groupe de vérification vidéo peut contenir jusqu'à quatre caméras, et chaque caméra dispose d'un lecteur associé (c'est à dire que le lecteur de la "porte principale" peut être associé à la "caméra de la porte principale").

Lorsqu'une transaction avec une carte connue est effectuée auprès d'un lecteur associé, l'image enregistrée du détenteur de carte ou du visiteur est affichée auprès de l'image prise en temps réel. Ceci permet à un garde de comparer les deux images pour vérifier l'identité de la personne. Par exemple:



Le système peut, si nécessaire, être mis en mode "Contrôle de la porte par PC" qui oblige le garde à sélectionner le bouton **Autoriser l'accès** ou **Interdir l'accès** pour chaque transaction.

Le premier champ sous les images affiche les informations concernant la transaction faite au niveau du lecteur, comme par exemple l'information si l'accès a été autorisé automatiquement, le numéro de carte (entre crochets) et la date et l'heure de la transaction.

Les trois champs restants peuvent afficher des données personnelles concernant la personne (comme le nom du gestionnaire de ligne), ou des informations au sujet du badge qui a été utilisé (telles que

ses dates d'activité et d'expiration). L'information affichée est spécifiée par l'écran Configuration/Vérification Vidéo.

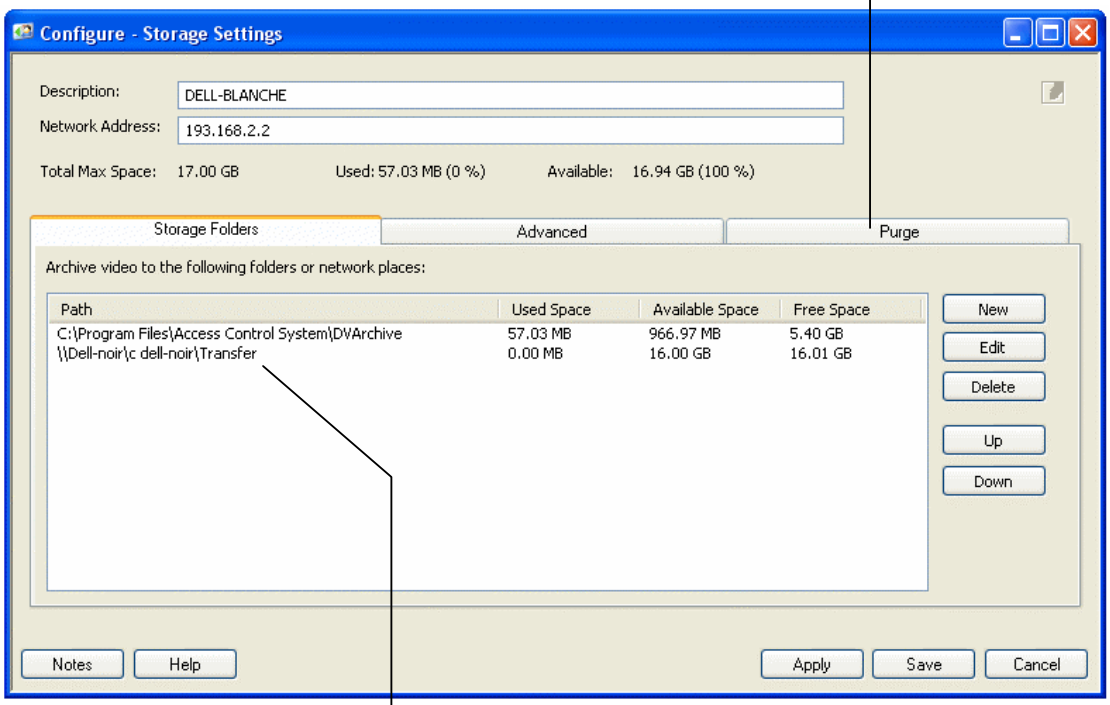
Logiciel de sauvegarde sur serveur vidéo

Le **Logiciel de sauvegarde sur serveur vidéo** est un système complet de gestion des données vidéo qui peut automatiquement sauvegarder des enregistrements pris par un système ENVS ou une caméra IP[3]. Il est possible d'enregistrer de la vidéo à partir des caméras IP seulement si le logiciel de sauvegarde sur serveur vidéo est installé.

Lors de l'utilisation de caméras ENVS, le logiciel permet aux enregistrements sauvegardés sur un ENVS d'être placés sur un lieu de stockage réseau ce qui libère de l'espace pour d'autres enregistrements et garanti que les enregistrements sont correctement archivés.

La configuration de la sauvegarde des données est paramétrée en utilisant l'écran Configuration/Vidéo numérique/Paramètres serveur de stockage, comme indiqué ci-dessous.

Vous pouvez paramétrer des horaires pour purger automatiquement les enregistrements, du dispositif de stockage réseau, qui sont plus anciens qu'un nombre de jours définis.



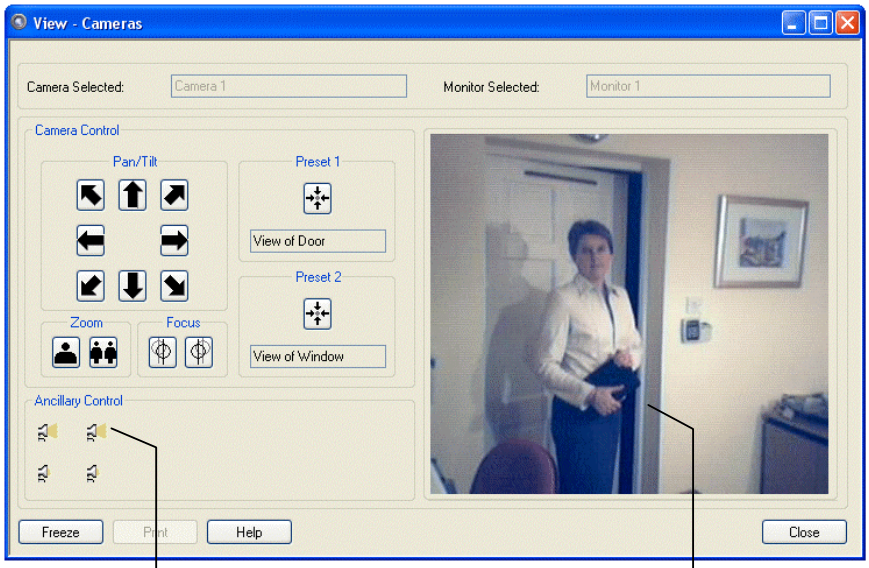
Il est possible de paramétrer de multiples emplacement de stockage pour enregistrer des vidéos à partir de chaque système ENVS. Si l'emplacement situé en haut de liste est complet, l'emplacement suivant est alors utilisé.

[3] IP cameras are available only with the full Digital Video Management Module.

Utiliser l' unités du connecteur et camerás CCTV

L'unité du connecteur dispose de connections pour les caméras et les moniteurs et est aussi capable de connecter des vidéos en temps réel de toutes les caméras connectées vers tous les moniteurs connectés. Un connecteur de caméras de télésurveillance est également capable de gérer la mise en marche ou l'arrêt des dispositifs auxiliaires tels que les lampes des caméras et les essuie-glaces.

Vous pouvez connecter des vidéos vers un moniteur sélectionné, contrôler la position de la caméra et mettre en marche ou arrêter les dispositifs auxiliaires en utilisant l'écran Affichage/ Caméras de surveillance comme indiqué ci-dessous. Des commandes alternatives peuvent être définies pour remplir des actions automatiques à des horaires définis ou en réponse à des alarmes ou événements.



Ces boutons mettent en marche ou arrêtent des dispositifs auxiliaires.

Si un connecteur a une connexion vidéo câblée vers un PC séparée, les images affichées sur le moniteur de surveillance vidéo sont aussi affiché ici.

Visualiser une vue CCTV pendant l’acquittement d’alarme

Un bouton spécial **Command** est intégré dans la fenêtre d’acquittement des alarmes. Il peut servir à commuter la caméra CCTV se trouvant à l’endroit d’alarme à un écran de contrôle prédéterminé. L’opérateur peut ainsi avoir un aperçu rapide et facile des images à l’endroit d’alarme. On peut installer la commande activée par le bouton **Command** dans la fenêtre Admin/Alarm/Commands.

Commandes vidéo numérique et commandes de commutateurs de vidéosurveillance

Les commandes suivantes sont disponibles à partir du logiciel SMS.

Commandes des caméras de surveillance vidéo

- Vidéos en temps réel - Affiche des vidéos en temps réel des caméras IP sélectionnées ou à partir des systèmes DVR et ENVS (ces commandes sont disponibles uniquement à partir de graphiques).
- Modification des paramètres vidéo - Modifie les paramètres de la caméra ENVS sélectionnée.
- Présélection PTZ - Place la caméra IP sélectionnée ou la caméra du système DVR ou ENVS dans une position prédéfinie.
- Enregistrement vidéo - Lorsqu'une alarme est déclenchée, la vidéo du système IP, DVR, ENVS est automatiquement enregistrée (pour les commandes à déclanchement uniquement).
- Remise à zéro des statistiques de bande passante - Remet à zéro les statistiques d'utilisation de la bande passante comme indiqué sur l'écran Affichage/Statut.
- Démarrage/Arrêt de l'enregistrement - Démarre/Arrête l'enregistrement du système IP, DVR, ENVS sélectionné.
- Connexion vidéo en temps réel - Connecte la vidéo en temps réel d'une caméra IP, DVR, ENVS à une cellule de l'écran Affichage/Vidéo numérique/Matrice virtuelle.
- Visionnage vidéo instantané - Affiche automatiquement une fenêtre contenant la vidéo enregistrée par une caméra IP, DVR ou ENVS.
- Mise en service/Mise hors service de la détection de mouvement - Met en service / hors service de la fonction de détection de mouvement pour une caméra ENVS.

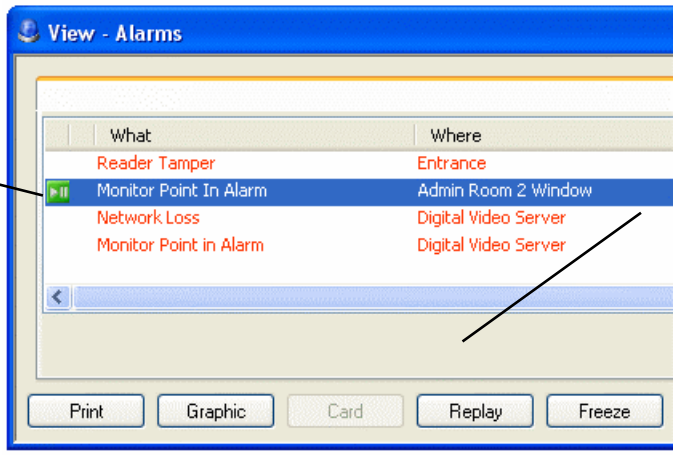
Commandes des commutateurs de caméra de télésurveillance

- Activer l'alarme - Entraîne le déclenchement d'une action préprogrammée au niveau du commutateur de la caméra de télésurveillance (Commande à déclenchement uniquement).
- Remise à zéro de l'alarme - Remet la commande d'alarme activée à zéro (Commande à déclenchement uniquement).
- Marche/Arrêt auxiliaire - Met le dispositif auxiliaire de la caméra de vidéosurveillance en marche /arrêt.
- Basculer sur le moniteur ou le nom de la caméra - Fait basculer la vidéo d'une caméra sélectionnée vers un moniteur CCTV sélectionné.

Visionnage d'alarmes et de rapports

Les enregistrements vidéo créés par une commande d'enregistrement vidéo (voir ci-dessus) peuvent être facilement visionnés à partir des écrans Affichage/Alarmes, Affichage/Activité ou Affichage/Historique/Activité. Par exemple

Chaque alarme qui a un clip vidéo associé, affiche cette icône dans l'écran Affichage/Alarmes



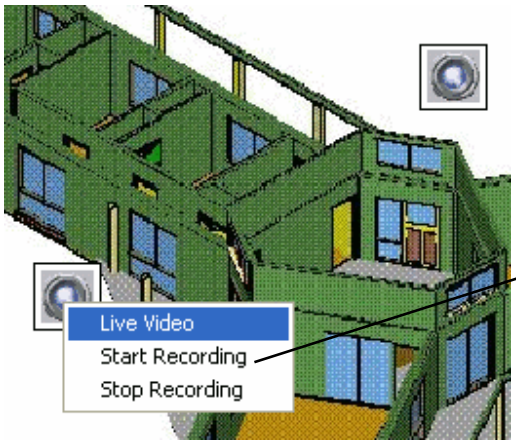
Vous pouvez visionner le clip vidéo en cliquant sur Visionnage.

Vous pouvez visionner le clip vidéo en cliquant sur Visionnage.

Intégration graphique

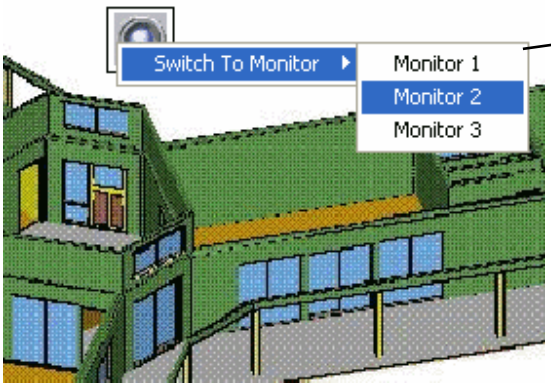
Les connecteurs de caméras IP, DVR, ENVS et de télésurveillance peuvent être ajoutés à des graphiques en utilisant l'écran Configuration/Graphique. Ajouter des caméras à un graphique vous permet de facilement localiser une caméra sur l'écran Affichage/Graphique et de visionner la vidéo en temps réel qui est prise par cette caméra.

Un clic droit sur une caméra IP, DVR ou ENVS dans l'écran Affichage/Graphique entraîne l'affichage des commandes suivantes:



Vous pouvez afficher des vidéos en temps réel à partir de la caméra ou démarrer/arrêter l'enregistrement.

Un clic droit sur un connecteur de caméra de surveillance entraîne l'affichage suivant:



Vous pouvez connecter l'image d'un connecteur de caméra de vidéo-surveillance vers le moniteur sélectionné.

Chapitre 7: La surveillance des alarmes

Comprendre la surveillance des alarmes

Toute action importante qui se passe sur des appareils tels que les lecteurs et les points de surveillance est classée ou parmi les événements ou parmi les alarmes. Les événements ne constituent pas de conditions sérieuses et sont simplement consignés pour les rapports futurs. Les alarmes pourtant (p.ex. le cas d'une porte forcée) constituent des violations potentiellement sérieuses de la sécurité et sont toujours affichées dans la fenêtre Alarms, qui est le noyau des capacités de surveillance d'alarmes du système.

Il est d'une importance incontournable que l'opérateur chargé de la surveillance des alarmes soit introduit dans le logiciel de gestion de sécurité ou qu'il ait ouvert la fenêtre de login. Le système devrait être réglé d'une manière à éviter tout autre scénario.

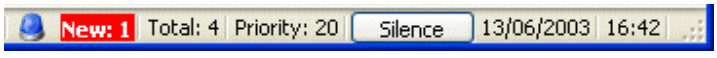
Comment les nouvelles alarmes sont signalées

Si une nouvelle alarme se produit, le PC ayant reçu ces alarmes émet un signal acoustique qui peut être varié selon la nature de l'alarme et sa source. Si la fenêtre de login est ouverte, les éléments d'alarme sont regroupés dans une case en bas au coin gauche du champ de dialogue:

La case indique le suivant:

- Le nombre des nouvelles alarmes, p.ex. le nombre des alarmes qu'on n'a pas encore acquittées. Vous apprendrez plus bas comment acquitter une alarme.
- Le nombre total des alarmes.
- La priorité de la nouvelle alarme étant d'une toute première importance (1 signifie la première priorité, 98 la dernière).

Au début de la session vous trouvez l'information suivante en bas du champ d'affichage ensemble avec un bouton **Silence** pour arrêter le son:



Dans le cas standard s'affiche „New Alarm!" à l'arrière-plan de la fenêtre de gestion de sécurité au moment qu'une nouvelle alarme se produit. De plus, on peut voir une lumière bleue clignotante dans

la barre des tâches du système Windows. Elle se meut vers le symbole d'une carte après que toutes les alarmes ont été acquittées.

Si votre système est conçu pour l'impression en temps réel, les éléments d'alarme sont imprimés automatiquement. C'est normal que l'on utilise une imprimante à impact qui fonctionne à papier continu à cette fin.

Votre système peut aussi être réglé d'une manière à ce qu'il affiche une vue en plan de l'endroit d'alarme ou qu'il envoie un courrier électronique à l'adresse d'une personne désignée.

Les démarches à prévoir en cas d'une alarme

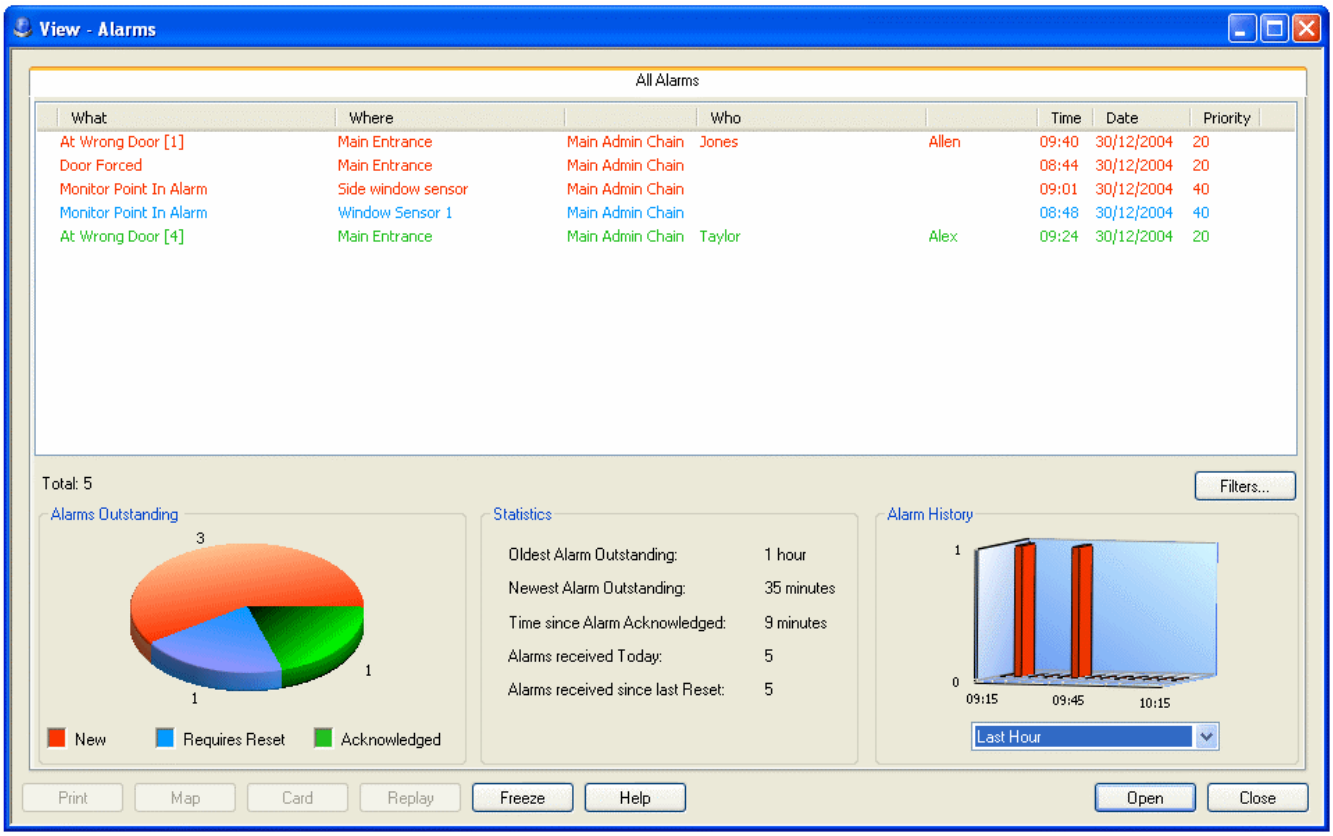
Lorsqu'une alarme se produit, les démarches suivantes s'imposent:

1. Regarder les détails de la nouvelle alarme dans la fenêtre View/Alarms.
2. Si des vues en plan ont été établies, regarder l'endroit de l'alarme (affichage automatique).
3. Acquitter l'alarme pour déterminer quelles instructions sont à donner par la suite, p.ex. contacter le gardien de la ronde qu'il aille à la recherche de l'origine.
4. Remettre à zéro l'alarme.
5. Effacer l'alarme dans la fenêtre Alarms.

Toutes les actions entamées sont enregistrées aux fins de rapports futurs. Les démarches énumérées ci-dessus sont décrites plus en détail dans les paragraphes ci-après.

Regarder les détails d'une alarme

En cas d'une nouvelle alarme on procédera d'abord à ouvrir la fenêtre Alarms à travers le menu View, si elle n'est pas toujours ouverte. La fenêtre Alarms donne des détails de toutes les alarmes qui n'ont pas encore été effacées. Exemple:



Dans le cas standard toutes les nouvelles alarmes sont représentées en rouge et par ordre de priorité. Le numéro de carte (si connu) est mis entre crochets. Les alarmes changent de couleur en allant du rouge au bleu ou vert au fur et à mesure des démarches de traitement effectuées, la signification des couleurs bleu et vert étant décrite dans les passages plus bas.

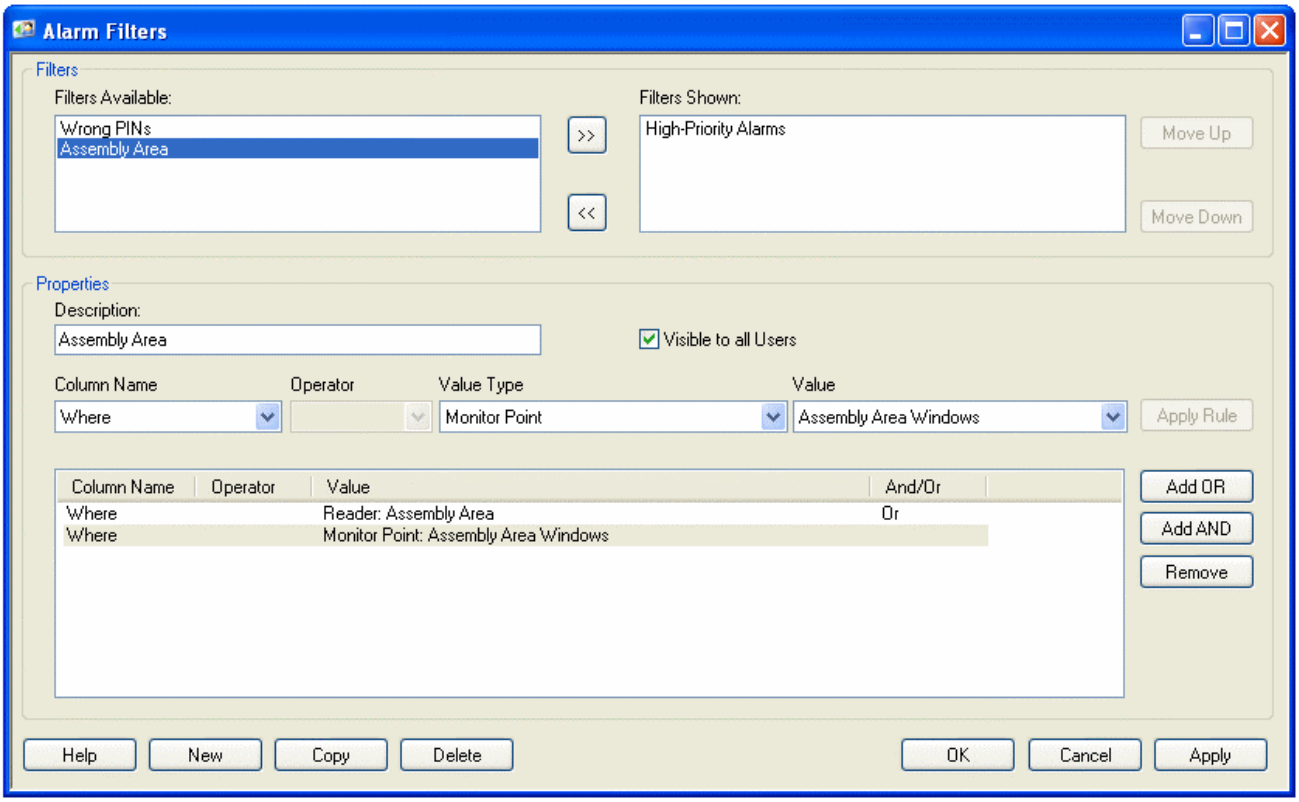
Pour chaque alarme il y a des détails concernant entre autres le nom de celui qui a causé l'alarme (s'il est connu d'après la carte utilisée), le message de l'alarme et l'endroit de son origine.

En option, dans la partie inférieure de l'écran sont affichés un diagramme camembert d'alarmes exceptionnelles, un panneau de statistiques d'alarmes et un diagramme en barres d'où on peut conclure quand des alarmes furent reçues. On peut changer le point de vue d'un diagramme en cliquant sur l'image et mouvant la souris.

Il est conseillé de tenir la fenêtre des alarmes toujours ouverte, car c'est comme ça qu'on peut lire les détails de nouvelles alarmes dès qu'elles s'annoncent.

Installer les filtres d'alarme

En cliquant sur le bouton **Filters** dans la fenêtre Alarms on voit s'afficher la fenêtre suivante dans laquelle on peut définir un ou plusieurs filtres d'alarme:



Chaque filtre que l'on définit crée un onglet à part dans la fenêtre Alarms. L'onglet visualise seulement ces alarmes pour lesquelles le filtre a été prévu. Chaque client du SMS peut afficher différents filtres d'alarme.

Les filtres d'alarme offrent une méthode de diviser la visualisation des alarmes dans la fenêtre Alarms. On peut, par exemple, créer un filtre d'alarme pour afficher seulement les alarmes d'un type spécifié ou d'un site spécialement choisi, ou la combinaison de différents types d'alarme.

Le panneau en bas de la fenêtre démontre comment le filtre d'alarme sélectionné en ce moment est installé. Dans cet exemple, le filtre "Assembly Area" affiche les alarmes reçues du lecteur de la zone de rassemblement ou de la fenêtre du point de surveillance de la zone de rassemblement.

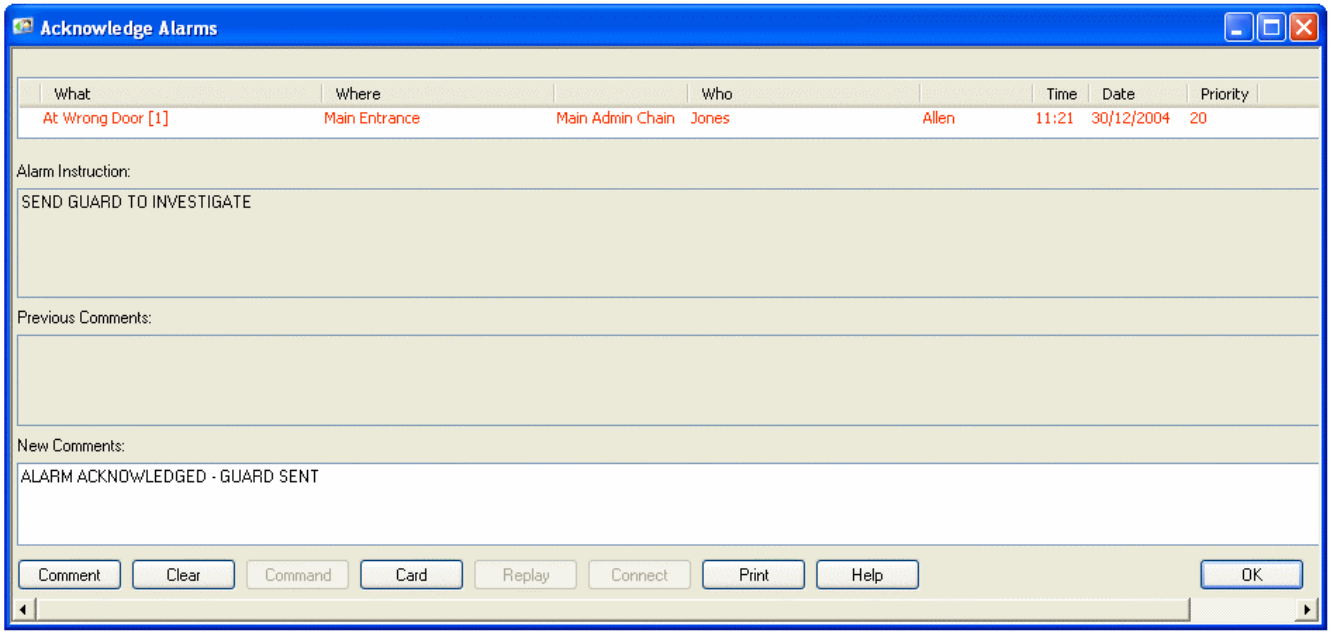
Regarder une vue en graphique de l'endroit d'alarme

Si des graphiques sont été définis pour votre installation, cliquez sur une alarme, sélectionnez ensuite le bouton **Graphique** pour afficher une vue en graphique de l'endroit d'alarme.

Des graphiques sont aussi toujours accessibles lorsqu'on sélectionne l'option **Graphiques** du menu View, ou on peut les faire afficher automatiquement (dans le menu Configure/Preferences).

Acquitter une alarme

On devrait acquitter une nouvelle alarme le plus vite possible après son déclenchement dans la fenêtre Acknowledge Alarms, comme c'est démontré dans la photographie d'écran ci-après. La fenêtre s' ouvre après un double-clic sur l'alarme dans la fenêtre Alarms, ou – si une vue en graphique est affichée – après l'appui sur le bouton **Acknowledge** dans la fenêtre **Graphique**.

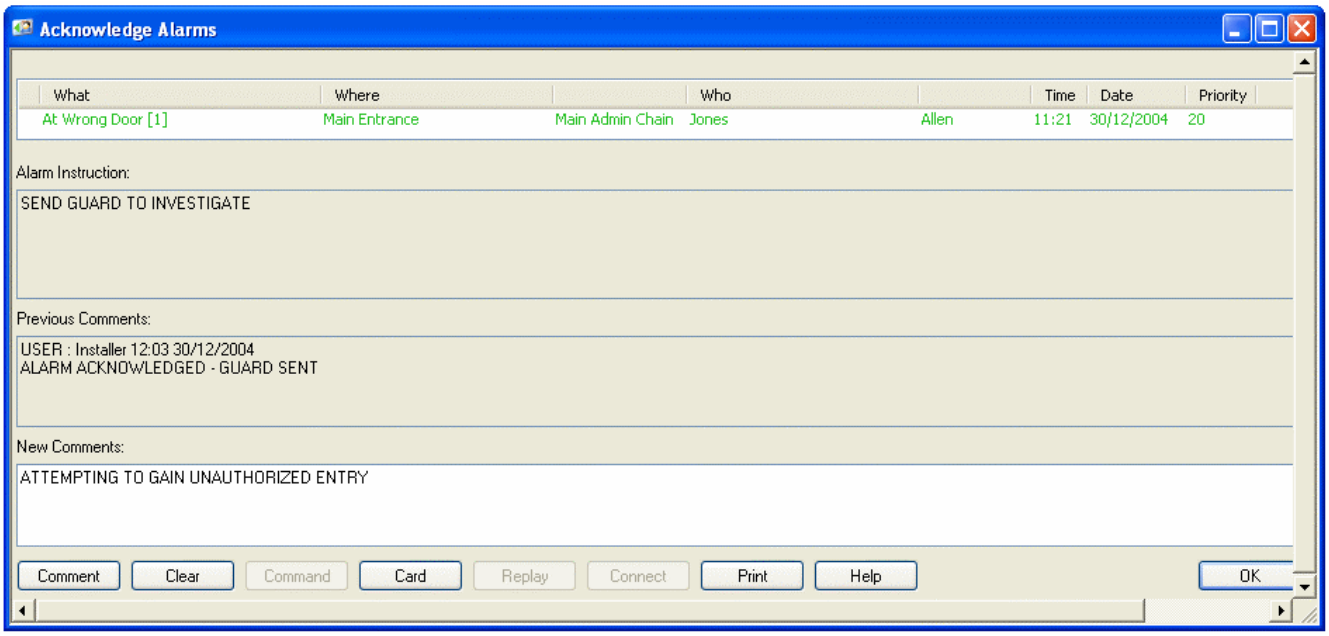


La fenêtre Acknowledge Alarms affiche les instructions auxquelles on devrait se tenir (dans ce cas, „SEND GUARD TO INVESTIGATE“ – envoyer un gardien à la recherche de l’origine d’alarme). Les instructions s’orientent spécifiquement vers le type d’alarme et sont à déterminer dans les fenêtres Admin/Alarm/Instructions et Admin/Alarm/Definitions.

La fenêtre Acknowledge Alarms offre aussi une case New Comments où l’on peut inscrire les mesures prises. On ajoute un commentaire ou en tapant un texte dans la case ou en cliquant sur le bouton **Comment** pour sélectionner l’un des commentaires prédéfinis. Les commentaires d’alarme préféfinis sont installés par un administrateur qui y procède par la fenêtre Admin/Alarm/Comments.

Après le clic sur **OK** l’alarme est aquittée et elle réapparaît dans la fenêtre Alarms, maintenant en bleu (c’est-à-dire que l’alarme est acquittée sans être remise à zéro) ou en vert (l’alarme peut être effacée). Ces états sont décrits dans les passages qui suivent.

Si besoin est, on peut retourner à la fenêtre Acknowledge Alarms pour ajouter encore plus de commentaires en sélectionnant à nouveau l’alarme dans la fenêtre Alarms. Les commentaires précédents sont lisibles dans la case Previous Comments, comme il est présenté ci-après.



Chaque commentaire dans la case Previous Comments est prédéterminé avec le nom de celui qui l'avait ajouté et l'heure de son introduction.

Le bouton **Command** est en état actif si une commande prédéfinie a été installée pour l'alarme dans la fenêtre Admin/Alarm/Commands. En cliquant sur le bouton, on lance la commande. Elle peut p.ex. projeter l'image CCTV de l'endroit d'alarme sur le moniteur CCTV, de sorte qu'on puisse voir la personne ayant causé l'alarme.

Réinitialiser l'alarme

Si tout le message d'alarme est affiché en bleu dans la fenêtre Alarms ou juste l'heure et la date, cela signifie qu'on a acquitté l'alarme, sans que l'unité n'ait été réinitialisée. Une sortie de secours où se trouve un point de surveillance n'a p.ex. pas été fermée. L'unité doit être remise à zéro avant qu'on ne puisse effacer la fenêtre Alarms.

Pour quelques-unes des alarmes, p, ex. les alarmes de carte, il n'y a pas d'état 'bleu'.

Effacer l'alarme

Si tout le message d'alarme est affiché en vert dans la fenêtre Alarms ou juste l'heure et la date, cela signifie qu'on a acquitté l'alarme et remis à zéro l'unité, si c'était nécessaire, mais qu'on ne l'a pas effacée dans la fenêtre.

On efface l'alarme en actionnant le bouton d'alarme (par lequel est affichée la fenêtre Acknowledge Alarm) et ensuite le bouton **Clear**. Il est peut-être souhaitable d'ajouter encore un commentaire avant l'effacement par **Clear**, p.ex. „Supervisor Notified" (responsable informé).

Chapitre 8: Produire des rapports

L’introduction

Les fonctions d’établir des rapports au sein du logiciel de gestion de sécurité permettent de rédiger à grande échelle des listes d’alarmes, d’événements, d’actions de l’utilisateur, de droits d’accès, de configurations installées et d’autres informations nécessaires à travers lesquelles on peut avoir un suivi de tous les renseignements essentiels.

Il est facile de produire grand nombre de différentes sortes de rapports. On peut p.ex. établir des rapports concernant les détenteurs de cartes ayant eu accès à des portes déterminées, concernant les gens ayant tenté d’entrer dans des zones qui n’étaient pas autorisées à l’accès et concernant les actions prises pour acquitter les alarmes.

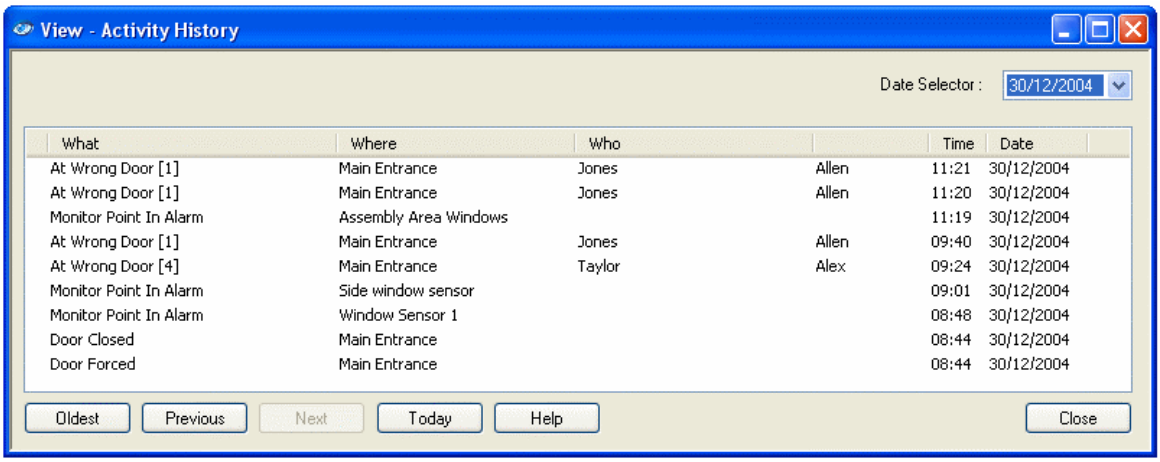
En utilisant les rapports fournis on peut rapidement retrouver les informations voulues. Les nombreuses options de filtrage sont une aide à afficher juste les informations requises, ce qui est plus clair à lire et plus facile à traiter.

Au surplus de sa flexibilité le système permet d’établir une bibliothèque de rapports définis par l’utilisateur qui peuvent être imprimés à intervalles réguliers. Pour l’adaptation ultimative du format et du contenu des rapports aux besoins de l’utilisateur, une possibilité est mise à disposition pour intégrer le logiciel populaire Crystal Reports®.

Le système de reporting est d’importance pour tous les directeurs qui doivent être sûrs qu’on peut enquêter correctement et rapidement sur les tentatives d’atteinte à la sécurité ou d’autres incidents ou qui ont besoin de dossiers exhaustifs au sujet de la configuration du système.

Les rapports d’activité

On peut avoir accès aux rapports d’activité à l’aide du menu View sur des PC-clients déterminés (comme installé dans la fenêtre Install/Clients). Ils sont affichés sur l’écran. Le rapport View/Activity signale toutes les alarmes et tous les événements dès qu’ils se produisent, et il y a un bouton **History** au moyen duquel on peut afficher n’importe quels alarmes et événements sur une base de quotidienneté qui ont été enregistrés dans le journal du système. Exemple:


View - Activity History
Date Selector :
30/12/2004
What
Where
Who
Time
Date
At Wrong Door [1] Main Entrance Jones Allen 11:21 30/12/2004
At Wrong Door [1] Main Entrance Jones Allen 11:20 30/12/2004
Monitor Point In Alarm Assembly Area Windows 11:19 30/12/2004
At Wrong Door [1] Main Entrance Jones Allen 09:40 30/12/2004
At Wrong Door [4] Main Entrance Taylor Alex 09:24 30/12/2004
Monitor Point In Alarm Side window sensor 09:01 30/12/2004
Monitor Point In Alarm Window Sensor 1 08:48 30/12/2004
Door Closed Main Entrance 08:44 30/12/2004
Door Forced Main Entrance 08:44 30/12/2004
Oldest
Previous
Next
Today
Help
Close

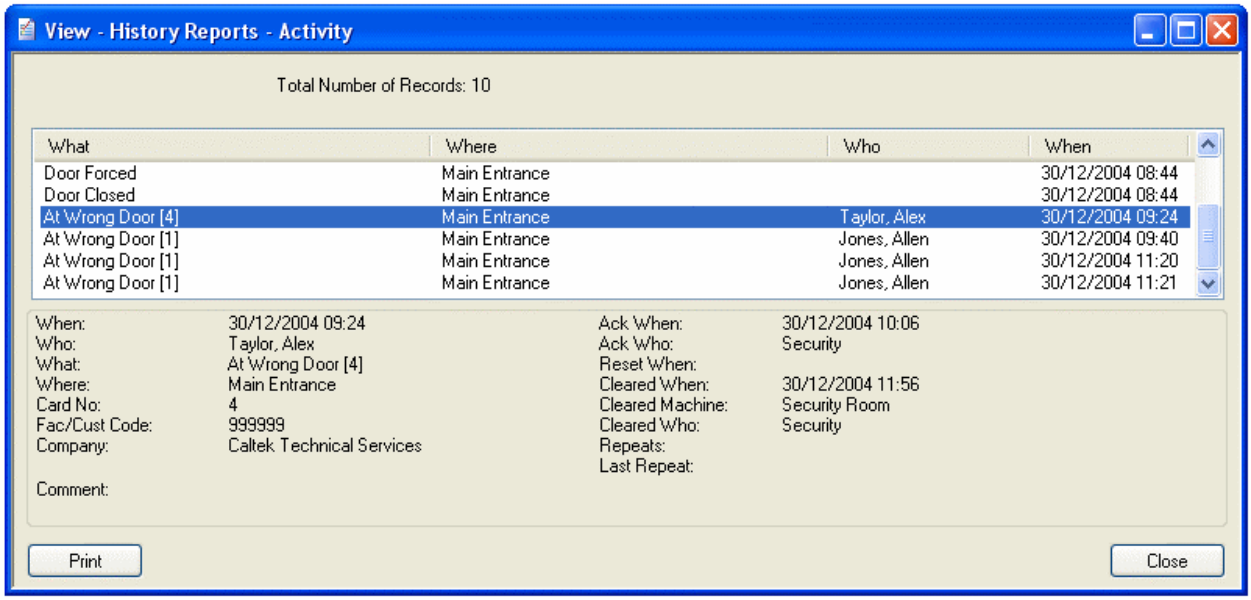
Les rapports d’événements

:

On peut exécuter différents types de rapports dans le menu View/History:

- **Activity** – „Activité“ pour réunir tous les détails des alarmes et événements précédents.
- **User Audit** – „Utilisateurs“ pour lister les actions précédentes retenues dans les fenêtres du logiciel de SMS.
- **Onsite Times** – „Temps au site“ pour lister la durée de présence des détenteurs de carte sur les lieux. Ce rapport peut p.ex. servir à vérifier les factures des sous-traitants.
- **Cardholders Onsite** – „Cartes de présence immédiate au site“ pour lister les cartes des détenteurs qui sont sur les lieux à un moment donné. Ce rapport pourrait être utile aux services de secours.
- **Patrols** – „Contrôle de ronde“ pour produire des informations sur les rondes des gardiens précédentes (Cf. le manuel *Guard Patrol Manager Installation & User Guide*). Le rapport fournit les détails du début et de la fin d’une ronde de contrôle et les infractions aux règles.
- **Système -** Permet d'examiner le contenu du livre de bord du système(Pour les ingénieurs uniquement).
- **Prédéfini -** Vous permet d'effectuer un rapport qui a été préalablement paramétré et personnalisé dans le menu Configurer/Rapports. Vous pouvez déclencher le rapport manuellement ou a des intervalles programmés. Les rapports pré-définis vous permettent de créer une librairie de vos rapports favoris, ce qui vous permet de gagner du temps si vous désirer avoir recourt fréquemment au même rapport.

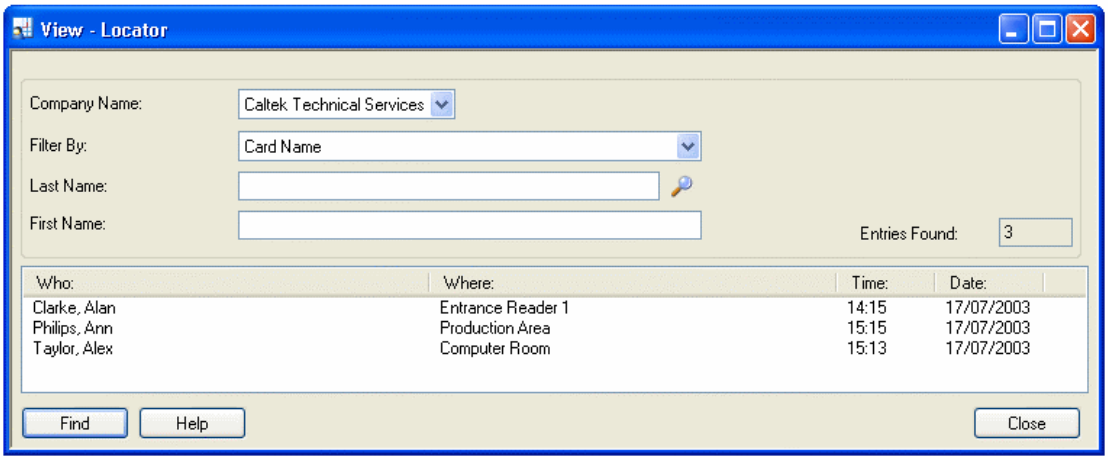
Ci-après un exemple d’un rapport d’activité, démontrant les alarmes et événements précédents.



Les rapports d'événements (Locator)

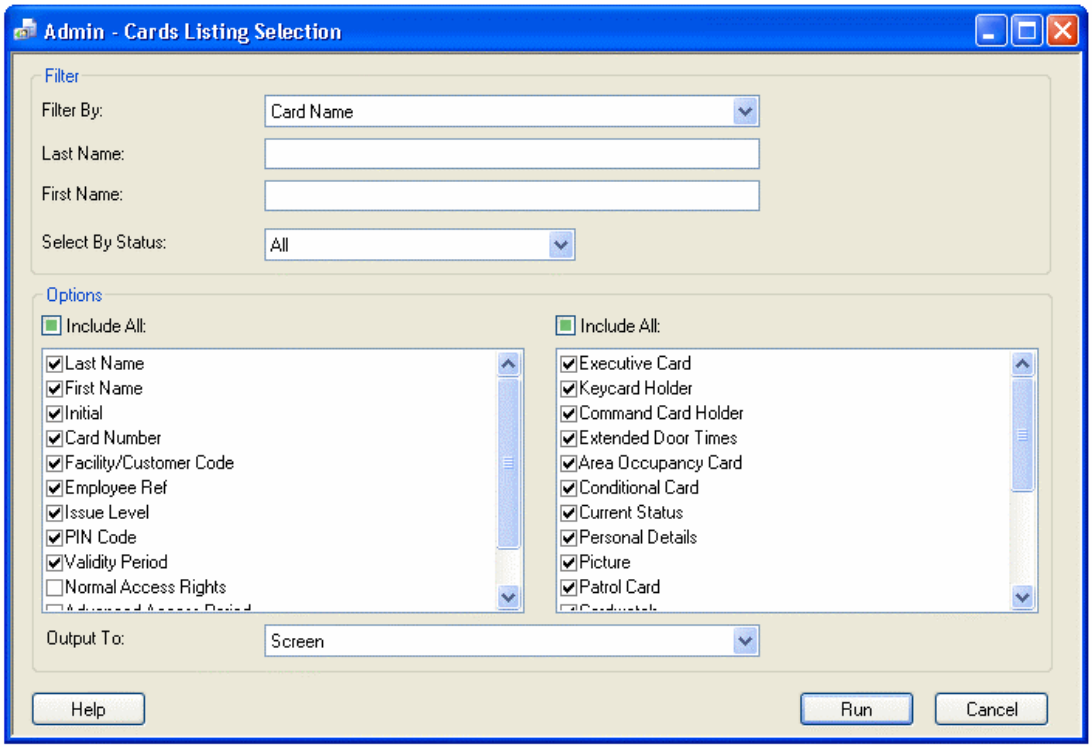
Il y a deux types de rapport de localisateur. Le premier est de fait un onglet de l'écran Détenteurs de cartes ou de l'écran Visiteurs, plus qu'un réel rapport. Ce rapport liste les 25 dernières transactions du détenteur de badge (Voir page **Error! Bookmark not defined.**).

Le second est accessible à partir du menu Affichage et affiche, pour chaque détenteur de cartes, le nom du lecteur et la dernière fois que un accès a été accordé. Ceci vous aide à déterminer le lieu actuel d'un ou plusieurs détenteur de cartes. Par exemple:



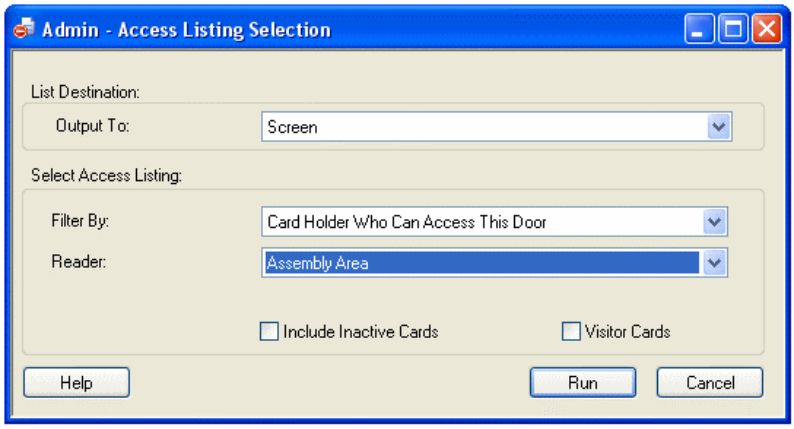
Rapports de cartes

L'écran Administration/Rapports/Cartes, vous permet de produire un rapport qui liste la façon dont des détenteurs de cartes sélectionnés on été paramétrés dans l'écran des détenteurs de cartes



Les rapports d’accès

Vous pouvez utiliser l'écran Admin/Reports/Access d’établir les rapports des droits d’accès:



En ouvrant le menu déroulant **Filter By**, on peut p.ex. établir des rapports comme suit:

- cartes utilisant un code de temps spécifié
- cartes utilisant un lecteur, un étage ou groupe de sorties spécifiés
- cartes pouvant utiliser une porte spécifiée
- portes auxquelles on peut avoir accès avec une carte spécifiée
- cartes à expiration entre des dates spécifiées

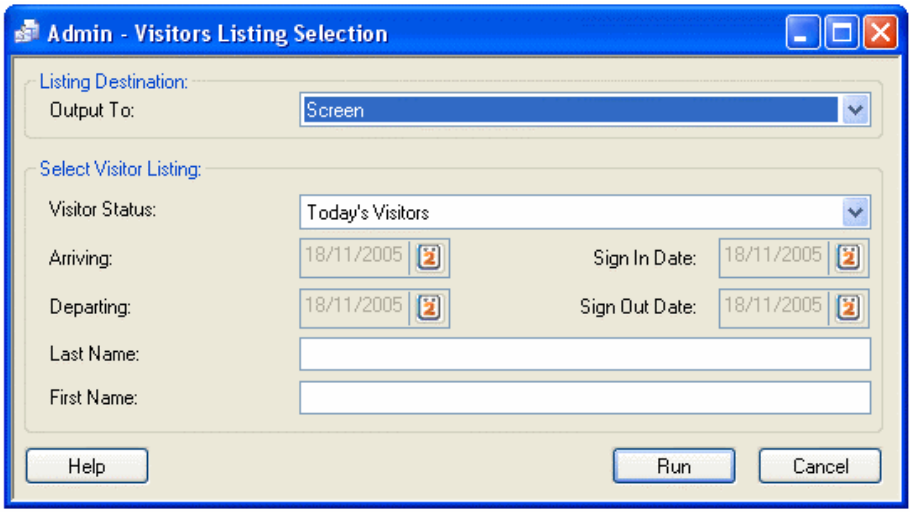
- cartes inutilisées durant un nombre de jours spécifié

Les rapports peuvent inclure ou exclure des cartes inactives et des cartes de visiteurs.

Rapports visiteurs

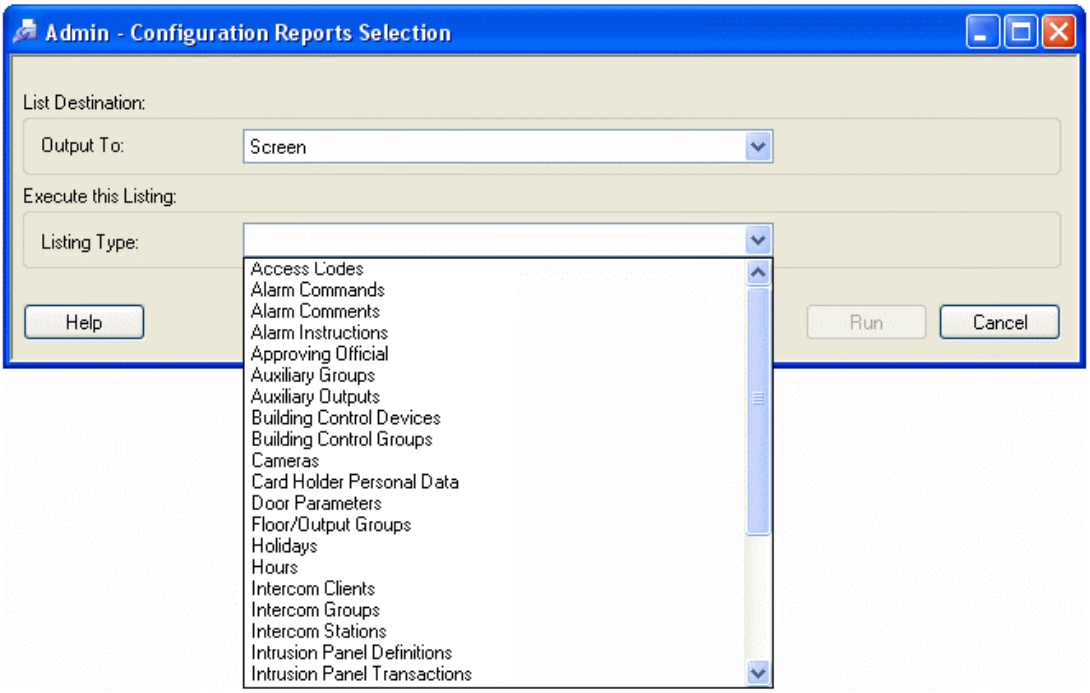
Le rapport Administration/Rapports/Visiteurs produit une liste des visiteurs passés, actuels et à venir. Vous pouvez vouloir utiliser ce rapport, par exemple pour trouver les noms de tous les visiteurs attendus à une date précise

:

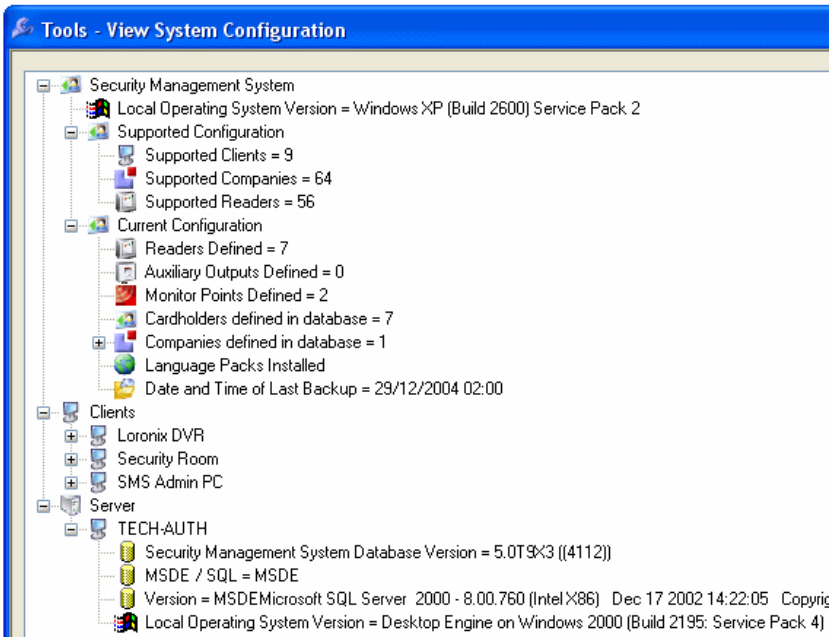


Rapports de configuration

Vous pouvez utiliser l'écran Administration/Rapports/Configuration pour produire un large nombre de rapports différents et voir la façon dont les lecteurs, les vacances, les codes horaires, les utilisateurs, les commandes, etc… ont été définies:



Vous pouvez aussi utiliser la fonction **Affichage Configuration Système** dans le menu des outils pour afficher une arborescence de la façon dont votre système a été paramétré, comme illustré sur l'image suivante:


Tools - View System Configuration
Security Management System
Local Operating System Version = Windows XP (Build 2600) Service Pack 2
Supported Configuration
Supported Clients = 9
Supported Companies = 64
Supported Readers = 56
Current Configuration
Readers Defined = 7
Auxiliary Outputs Defined = 0
Monitor Points Defined = 2
Cardholders defined in database = 7
Companies defined in database = 1
Language Packs Installed
Date and Time of Last Backup = 29/12/2004 02:00
Clients
Loronix DVR
Security Room
SMS Admin PC
Server
TECH-AUTH
Security Management System Database Version = 5.0T9X3 ((4112))
MSDE / SQL = MSDE
Version = MSDEMicrosoft SQL Server 2000 - 8.00.760 (Intel X86) Dec 17 2002 14:22:05 Copyrig
Local Operating System Version = Desktop Engine on Windows 2000 (Build 2195: Service Pack 4)

Les rapports de présence (roll call)

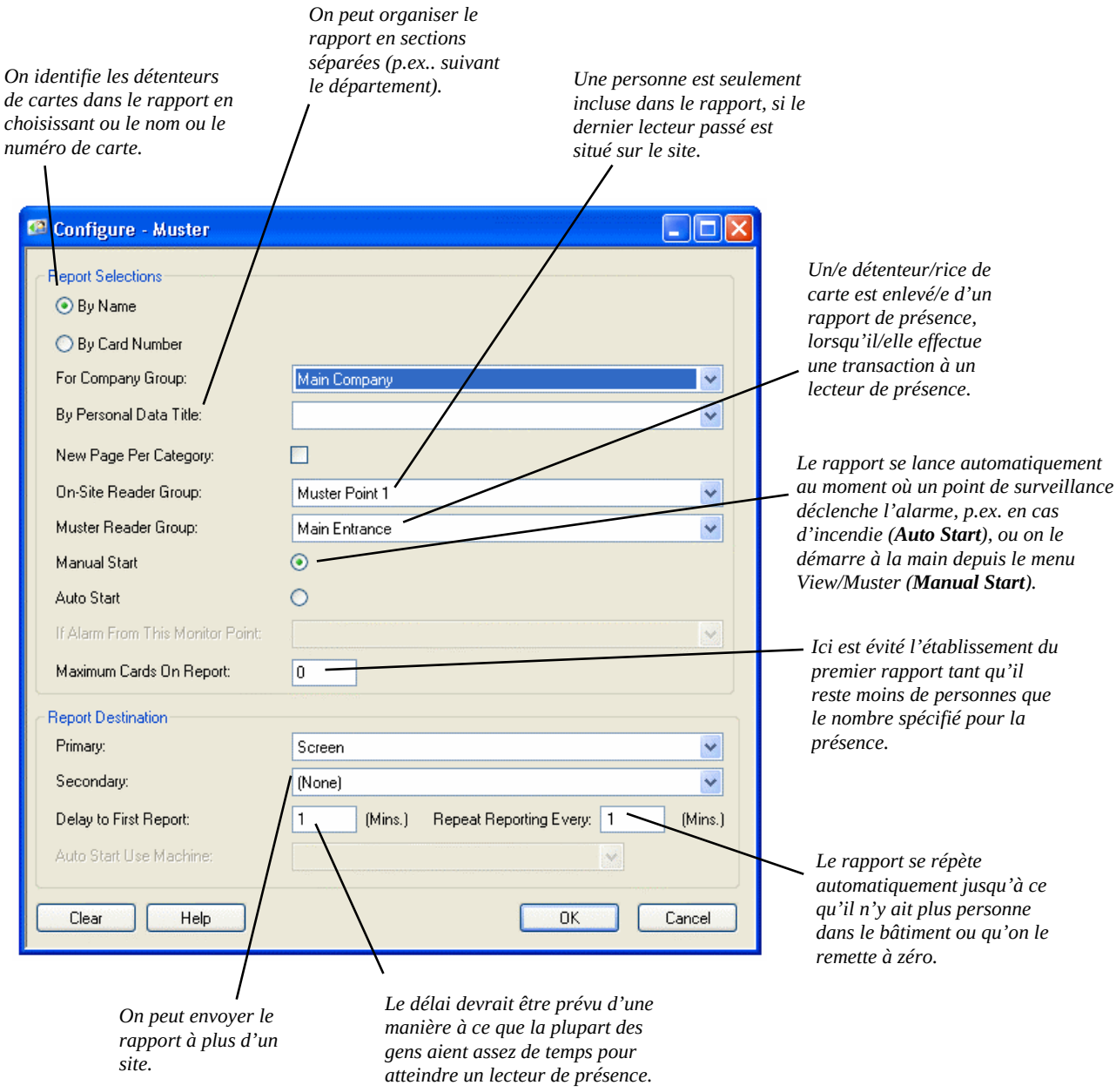
Un rapport de présence (disponible seulement avec le module „Safety Roll Call Management“) démontre une liste de ces gens que le logiciel de gestion de sécurité avait enregistrés comme étant présents dans le bâtiment, en commun avec les détails du dernier lecteur qu’ils avaient franchi. La liste est prévue comme une aide pour les services de sauvetage dans un cas d’incendie ou d’autres cas d’urgence. Voici un exemple d’un rapport de présence:

Last Name:	First Name:	Card Number:	Reader Description:	Time:	Date:
Booth	Alan	0025	Processing Room	09:01	12/8/04
Burrows	Belinda	0029	Processing Room	08:56	12/8/04
Corfield	David	0135	Stores 1	08:47	12/8/04
Fendick	Robert	0119	Computer Room	07:32	12/8/04
Kelsey	Sarah	0098	Processing Room	08:45	12/8/04
				TOTAL:	5

Les rapports de présence peuvent être établis automatiquement au moment où un point de surveillance réagit comme s’il y avait une alarme d’incendie. On peut les établir aussi à la main par la fenêtre View/Muster.

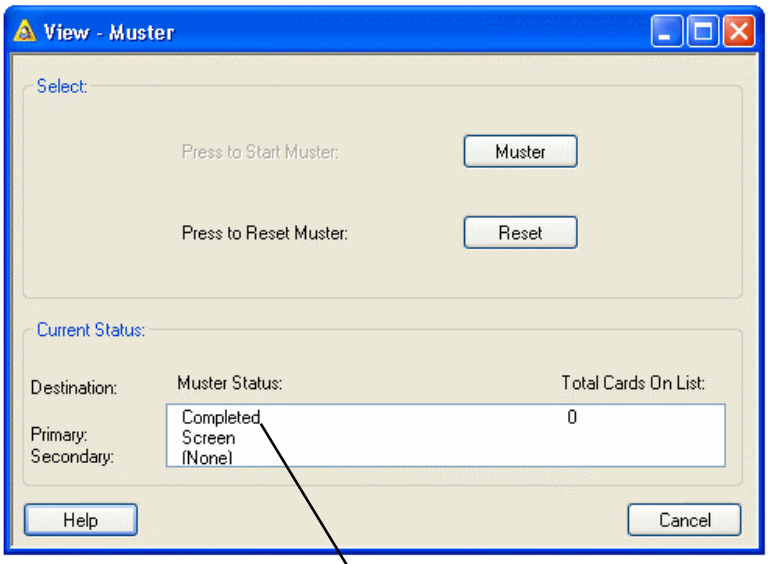
La configuration des rapports de présence

Le rapport de présence doit d'abord être installé dans la fenêtre Configure/Muster:


On identifie les détenteurs de cartes dans le rapport en choisissant ou le nom ou le numéro de carte.
On peut organiser le rapport en sections séparées (p.ex.. suivant le département).
Une personne est seulement incluse dans le rapport, si le dernier lecteur passé est situé sur le site.
Un/e détenteur/rice de carte est enlevé/e d'un rapport de présence, lorsqu'il/elle effectue une transaction à un lecteur de présence.
Le rapport se lance automatiquement au moment où un point de surveillance déclenche l'alarme, p.ex. en cas d'incendie (Auto Start), ou on le démarre à la main depuis le menu View/Muster (Manual Start).
Ici est évité l'établissement du premier rapport tant qu'il reste moins de personnes que le nombre spécifié pour la présence.
Le rapport se répète automatiquement jusqu'à ce qu'il n'y ait plus personne dans le bâtiment ou qu'on le remette à zéro.
On peut envoyer le rapport à plus d'un site.
Le délai devrait être prévu d'une manière à ce que la plupart des gens aient assez de temps pour atteindre un lecteur de présence.
Configure - Muster
Report Selections
By Name
By Card Number
For Company Group:
Main Company
By Personal Data Title:
New Page Per Category:
On-Site Reader Group:
Muster Point 1
Muster Reader Group:
Main Entrance
Manual Start
Auto Start
If Alarm From This Monitor Point:
Maximum Cards On Report:
0
Report Destination
Primary:
Screen
Secondary:
(None)
Delay to First Report:
1
(Mins.)
Repeat Reporting Every:
1
(Mins.)
Auto Start Use Machine:
Clear
Help
OK
Cancel

Surveiller le contrôle de présence

On peut surveiller le processus du contrôle de présence depuis la fenêtre View/Muster, comme c'est présenté ci-après. La fenêtre fournit un aperçu immédiat du nombre des gens se trouvant sur le site et de l'état du contrôle de présence.



*Lorsqu'on sélectionne une option comme **Détenteurs de cartes** dans le menu d'admin., une autre fenêtre apparaît dans la zone principale de*

On devrait veiller à ce que le nombre des gens inclus dans chaque nouveau rapport se réduise. Ceci s'explique par le fait que, tant qu'une personne fait une transaction à un lecteur de présence ou à tout autre lecteur qui n'est pas situé sur le site, elle est enlevée du prochain rapport.

Le système ignore une transaction à un lecteur, si une alarme/un événement „porte non ouverte" ont été générés.

Le cas d'urgence (ou d'exercice) terminé il faut réinitialiser le contrôle de présence dans la fenêtre View/Muster. Pendant la réinitialisation on peut sélectionner un lecteur; le système assume une transaction automatique sur ce lecteur pour tous ceux, dont le dernier lecteur passé a été un lecteur du contrôle de présence. Ceci permet de reprendre tout le monde dans un autre rapport de présence, à condition qu'il soit démarré aussitôt après la remise à zéro.

Chapitre 9: D’autres fonctions

Le chapitre décrit diverses autres fonctions importantes du logiciel de gestion de sécurité.

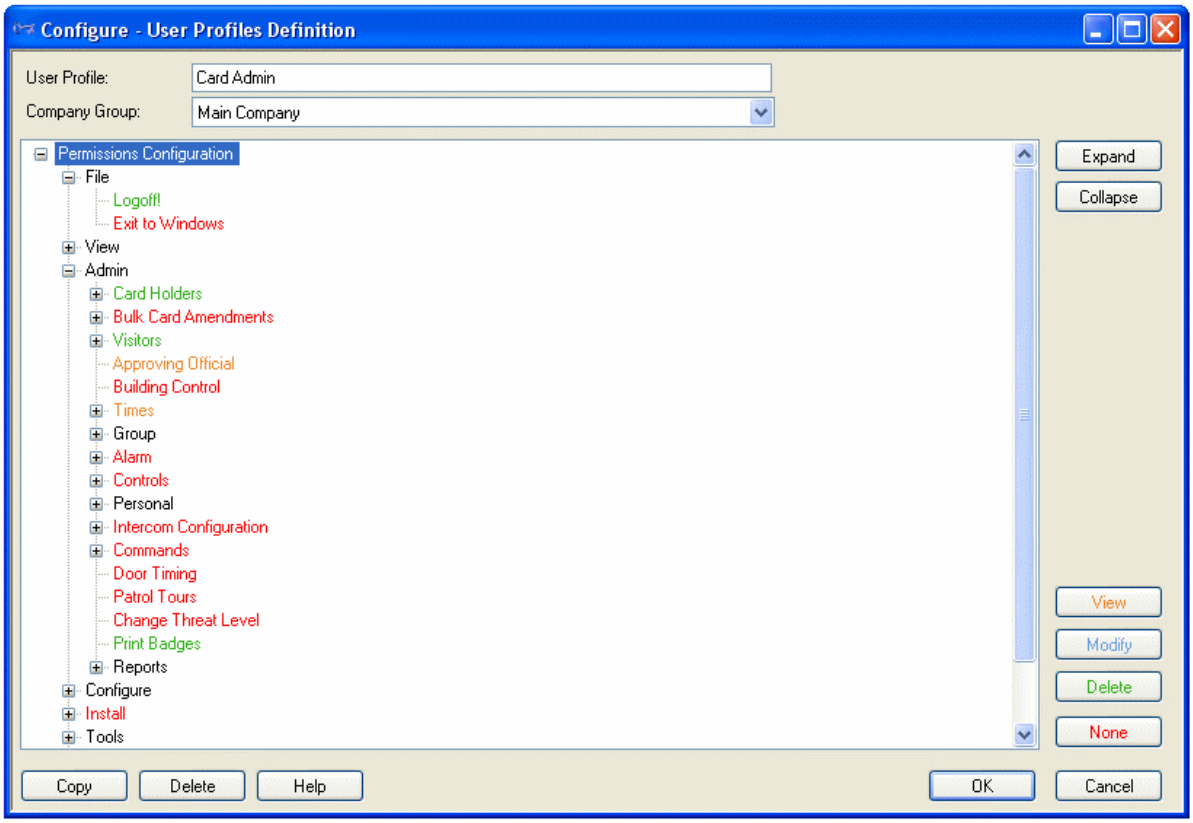
Installer les profils d’utilisateurs et les comptes

Un utilisateur est une personne qui se sert du logiciel de gestion de sécurité sur l’ordinateur. Il y a deux démarches pour installer les utilisateurs:

1. Utiliser la fenêtre Configure/User/Profiles pour définir un ou plusieurs profils d’utilisateurs. Chaque profil comprend un nombre de droits pour les fenêtres du logiciel de gestion de sécurité.
2. Utiliser la fenêtre Configure/User/Accounts pour créer le compte d’utilisateur où sont spécifiés le nom de login de l’utilisateur, le mot de passe et le profil.

Installer les profils

Les profils sont installés dans la fenêtre Configure/User/Profiles:



Un profil détermine un nombre de droits d'accès aux fenêtres du logiciel de gestion de sécurité. On peut installer une série de profils pour différentes catégories d'utilisateurs. Dans l'exemple de la page précédente, le profil est désigné de „Card Admin Permissions", ce qu'on peut assigné à chaque utilisateur qui a à assumer des tâches d'administration de carte dans le logiciel de gestion de sécurité.

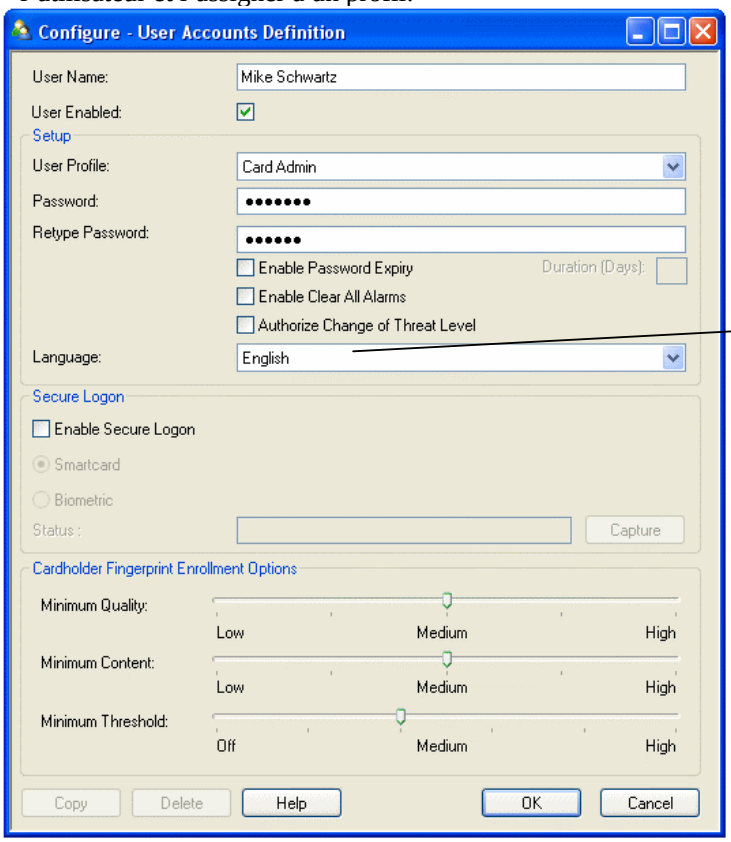
Chaque profil dispose de quatre niveaux d'accès à chaque fenêtre: None – néant (rouge), View – vue (orange), Modify – modifier (bleu) et Delete – effacer (vert). Si l'on met p.ex. l'accès à une fenêtre à la seule vue, les utilisateurs appartenant au profil peuvent lire le contenu de la fenêtre, mais n'y peuvent rien faire d'autre. L'accès à „Modify" permet aux utilisateurs d'apporter des modifications aux informations de la fenêtre, et l'accès à „Delete" est une possibilité pour les utilisateurs de supprimer des enregistrements entiers, p.ex. la définition d'un détenteur de carte.

Par les profils on peut restreindre la résalisation de tâches pour chaque type d'utilisateur, ce qui améliore non seulement la sécurité du système, mais simplifie aussi l'interface utilisateur, car le système affiche les options de menu pour les seules fenêtres auxquelles l'utilisateur a un accès. Les profils facilitent l'installation des privilèges de nouveaux utilisateurs ou la modification de ceux concédés aux utilisateurs existants.

Comme c'est le cas pour la plupart des systèmes d'ordinateur qui offrent ces types d'organisation de sécurité, on devrait admettre un seul utilisateur ayant l'accès à toutes les options (et, si applicable, aux informations de chaque société).

La création d'un compte d'utilisateur

Dans la fenêtre Configure/User/Accounts on peut créer le nom de login et le mot de passe de l'utilisateur et l'assigner à un profil:



S'il y a différents paquets de langues SMS installés, on peut choisir celle qui convient aux besoins de l'usager. Au moment de l'ouverture de la session les menus et options s'affichent dans la langue spécifiée.

Par une simple sélection du profil (dans la fenêtre **User Group**) les droits nécessaires de l'utilisateur s'installent immédiatement.

Les options **Secure Logon** assurent la possibilité qu'un utilisateur n'est accepté qu'après avoir présenté une carte à mémoire ou l'empreinte digitale à un lecteur approprié. Les options **Cardholder Fingerprint Enrollment Options** sont utilisées lorsqu'il y a des empreintes digitales enregistrées dans les fenêtres Admin/Card Holders ou Admin/Visitors.

Transmettre des commandes

La possibilité d'envoyer des commandes est une fonction très puissante du système de gestion de sécurité, grâce à laquelle on peut changer l'état et le mode de service des appareils comme lecteurs, points de surveillance, sorties auxiliaires et unités de commutation CCTV.

Il y a trois types de commandes:

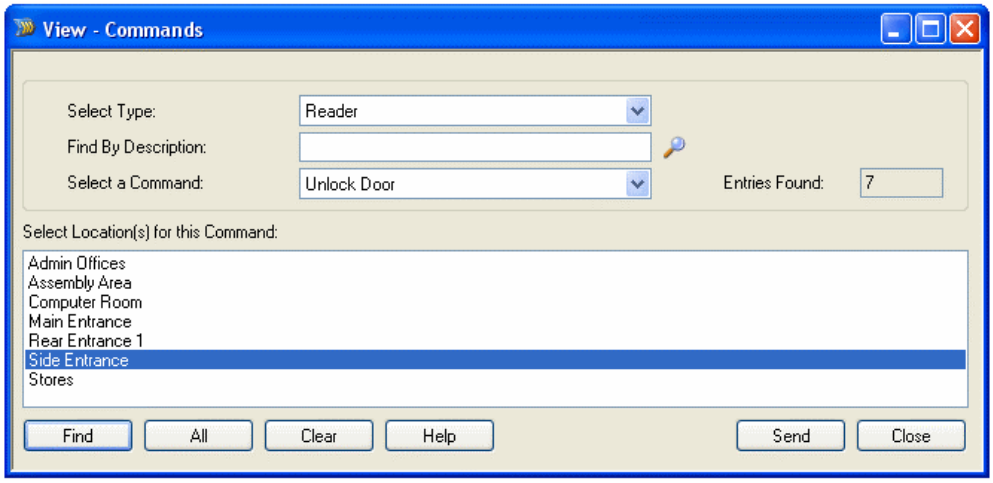
- **Manual Commands** (commandes manuelles) – Ceci permet de changer immédiatement l'état ou le mode de service d'un appareil. On peut p.ex. envoyer une commande manuelle pour déverrouiller une porte ou commuter un lecteur du mode „card-only" (carte seulement) au mode „card-and-PIN" (carte et PIN).
- **Scheduled Commands** (commandes programmées) – Ce sont des commandes à exécuter chaque jour à des temps prédéterminés. On pourrait p.ex. installer des commandes programmées pour enregistrer des vidéos CCTV chaque soir à la même heure.
- **Conditional Commands** (commandes de déclenchement) – Une commande de déclenchement est seulement réalisée lorsqu'une action prédéterminée a lieu. On pourrait p.ex. commuter une caméra CCTV à un écran de client SMS, lorsqu'un capteur déclenche une alarme ou les portes ne se déverrouillent pas à cause d'une alarme d'incendie. Les commandes de déclenchement sont également connues comme des opérations conditionnelles „If, Then, When" (SI, ALORS, QUAND).

Les passages suivants expliquent plus en détail les différents types de commandes.

La possibilité de transmettre une commande unique à un groupe de points de surveillance, de lecteurs ou de sorties auxiliaires est une fonction qui épargne du temps (créée à utiliser les options du menu Admin/Group). La commande est alors exécutée sur tous les appareils du groupe.

Les commandes manuelles

On peut envoyer des commandes manuelles en sélectionnant l'option **Commands** du menu View. Toute commande envoyée est exécutée immédiatement. Dans l'exemple suivant une commande a été passée pour déverrouiller la porte à l'entrée latérale.

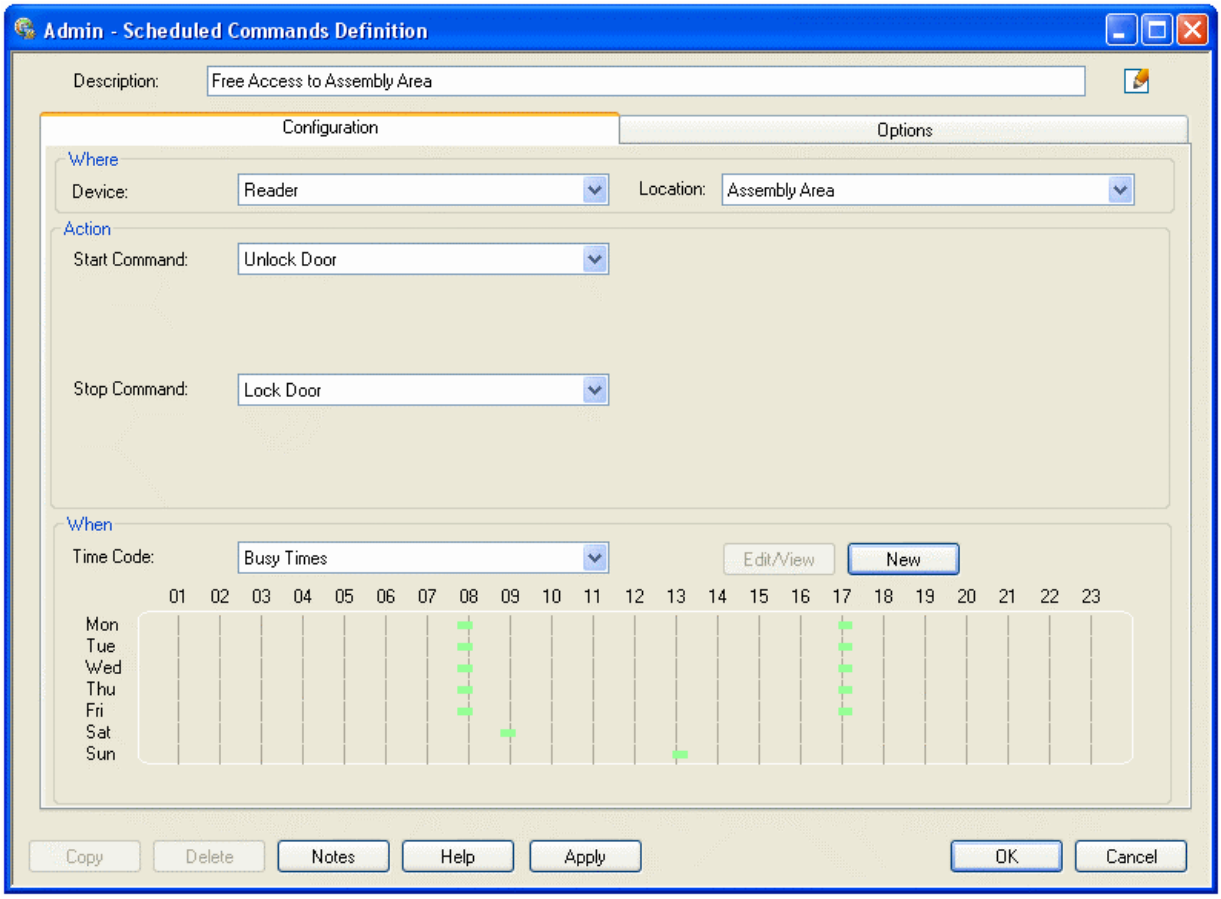


On peut aussi envoyer des commandes à la main depuis les fenêtres View/Status et View/Graphiques.

On peut restreindre les commandes manuelles que les usagers peuvent recevoir des fenêtres View/Commands, View/Graphiques et View/Status après avoir installé les commandes prédéfinies dans la fenêtre Admin/Commands/Predefined.

Les commandes programmées

Les commandes programmées s'installent par la fenêtre Scheduled Commands (Admin/Scheduled). Exemple:



Les commandes programmées consistent en une paire de commandes et un code de temps. On désigne l'une des commandes pour le départ et l'autre pour l'arrêt. La commande de départ est alors exécutée à chaque moment de départ et la commande d'arrêt à chaque moment d'arrêt.

Regardons l'exemple suivant qui reflète la commande programmée installée dans la figure précédente:

Time code (Code de temps) ("Busy Times" – heures de pointe):

de 07h45 à 08h05 de lundi à vendredi

de 16h55 à 17h15 de lundi à vendredi

de 08h45 à 09h05 les samedis seulement

de 12h55 à 13h15 les dimanches seulement

C**ommande de départ:** déverrouiller la porte

C**ommande d'arrêt:** verrouiller la porte

Cet exemple démontre une commande programmée qui pourrait servir à déverrouiller et reverrouiller la porte d'entrée principale vers la zone de rassemblement à des heures très fréquentées de la journée. La commande de départ signifie de déverrouiller la porte, ce qui permet aux gens d'accéder à la porte sans devoir présenter leurs cartes. La commande est exécutée à 7h45 et à 16h55 de lundi à vendredi, à 8h45 les samedis et à 12h55 les dimanches.

La commande d’arrêt signifie de reverrouiller la porte, c’est-à-dire que les gens arrivant après cette commande peuvent avoir accès de la manière régulière, donc en présentant une carte au lecteur. La commande est exécutée à 8h05 et 17h15 de lundi à vendredi, à 9h05 les samedis et à 13h15 les dimanches.

C’est normal, qu’on obtient comme dans l’exemple précité des effets contraires pour les commandes de départ et d’arrêt.

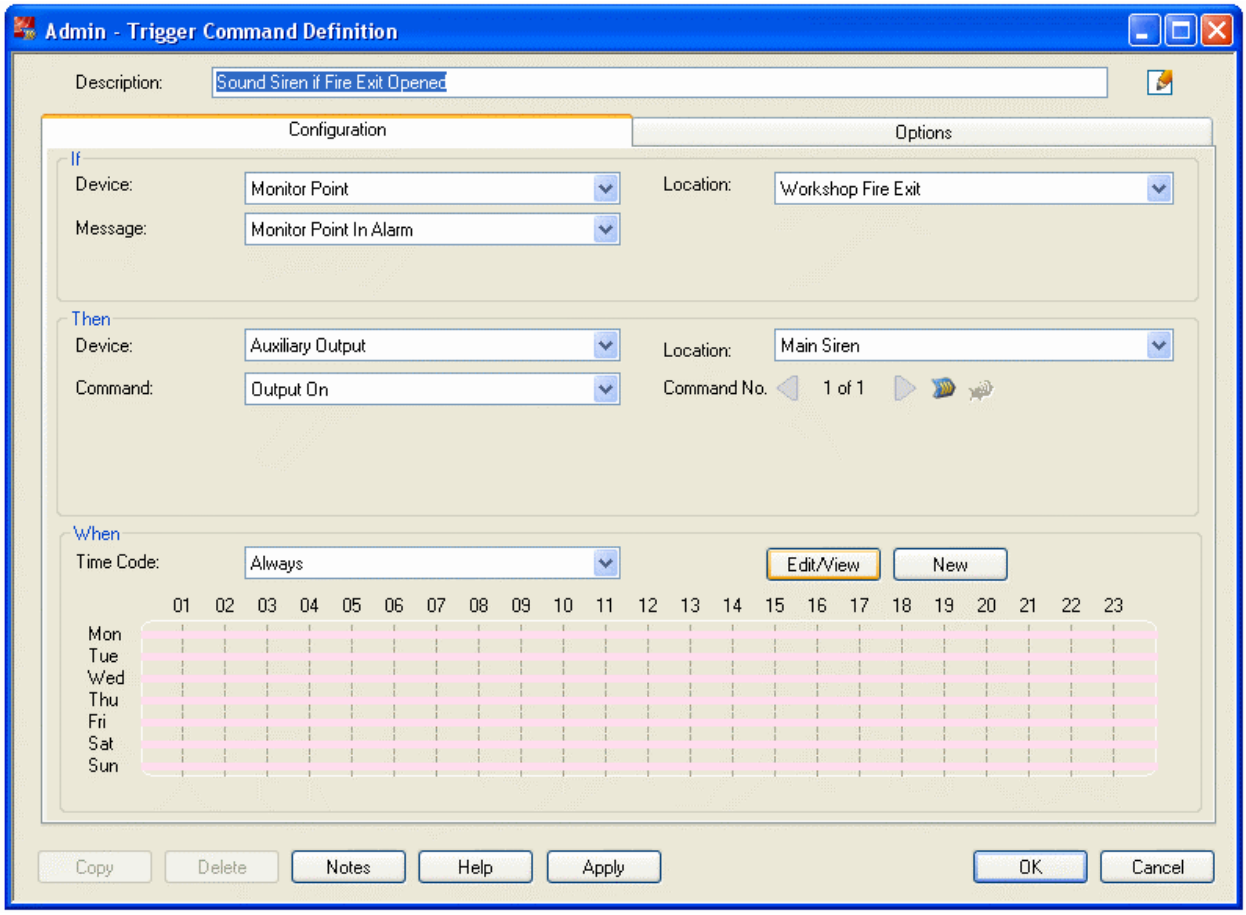
Des commandes programmées peuvent également être utiles pour commuter des lecteurs en différents modes. Peut-être veut-on prévoir, comme une mesure de sécurité en plus, la commutation des lecteurs en mode de carte et PIN pendant la nuit.

On peut également activer et désecativer un point de surveillance ou un groupe de points de surveillance, ce qui peut être utile, si les gens veulent p.ex. laisser ouvertes dans la journée les sorties de secours surveillées.

Une sortie auxiliaire ou un groupe de sorties auxiliaires peuvent également être mise en ou hors service suivant l’heure du jour, ce qui s’approprie pour l’éclairage extérieur ou d’autres appareils.

Les commandes de déclenchement

Les commandes programmées promettent une grande flexibilité pour la mise en œuvre du système de gestion de sécurité, mais il devient encore plus flexible grâce à l’emploi de commandes de déclenchement (aussi connues sous le nom de commandes conditionnelles), comme paramétré dans l'écran Administration/Commandes Déclencheur (Admin/Conditional Commands). La figure ci-après présente un exemple d’une commande de déclenchement, qui est exécutée, lorsque le point de surveillance „Workshop Fire Exit“ (sortie de secours de l’atelier) est en état d’alarme.



Une commande de déclenchement (trigger command) est exécutée, lorsqu'un message spécifié d'alarme/événement est généré par un appareil/une carte indiqués entre un temps de départ et un temps d'arrêt d'un code de temps déterminé. Ceci devient plus clair par un exemple simple! Figurez-vous la commande de déclenchement de la figure précédente:

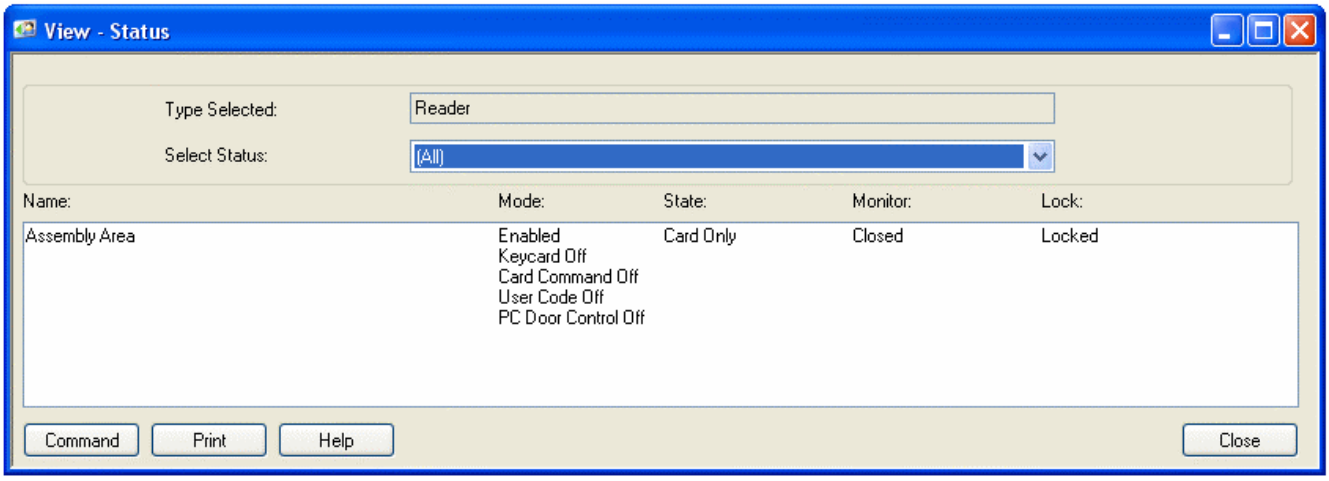
Nom d'appareil:	Sortie de secours de l'atelier (un point de surveillance)
Message d'alarme/d'événement:	Point de surveillance en état d'alarme
Commande:	Sortie en service
Commande à:	Sirène principale (une sortie auxiliaire)
Code de temps:	toujours

Dans cet exemple la sirène principale retentit, dès qu'à n'importe quel moment le point de surveillance à la sortie de secours de l'atelier génère l'alarme/l'événement „Monitor Point in Alarm".

Dans ce cas la commande conditionnelle est déclenchée comme résultat d'une alarme/d'un événement survenus à un point de surveillance, mais il est également possible que les commandes conditionnelles se déclenchent p.ex. suite à une alarme/un événement d'un lecteur ou d'une carte. En outre, si l'on choisit un groupe de moniteurs ou de lecteurs, la commande est déclenchée, lorsque n'importe quel appareil du groupe génère l'alarme/l'événement sélectionnés.

Regarder l’état des appareils

L’option **Status** du menu View permet d’avoir à un moment donné un aperçu de l’état et du mode de service des appareils tels que lecteurs, points de surveillance et sorties auxiliaires. Exemple:

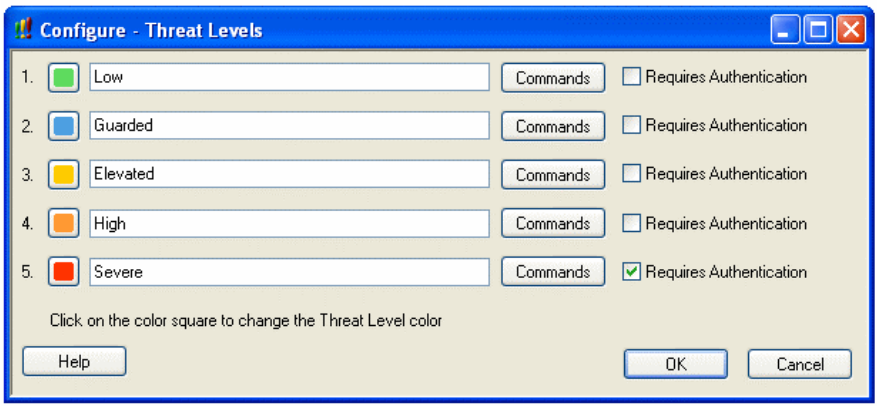


L’exemple présente l’état du lecteur installé dans le lieu de montage.

L’option **Status** permet la surveillance d’appareils en temps réel, ce qui signifie que toute modification d’informations qu’on est en train de regarder est affichée immédiatement, de sorte qu’on n’ait pas à sortir de et à ré-entrer dans la fenêtre.

La gestion du niveau de risque

Les caractéristiques optionnelles de la gestion du niveau de risque du système de gestion de sécurité permettent de changer la sécurité d’un bâtiment par l’actionnement d’un bouton. On peut d’une part accroître la sécurité s’il y a un risque plus élevé d’activités criminelles ou terroristes, ou même pendant des périodes d’occupation limitée, p.ex. pendant les vacances ou fermetures provisoires, et d’autre part on peut réduire la sécurité pendant d’autres périodes. On peut avoir cinq niveaux de risque, dont chacun peut être adapté aux besoins du client dans la fenêtre Configure/Threat Levels pour assurer différents niveaux de sécurité:

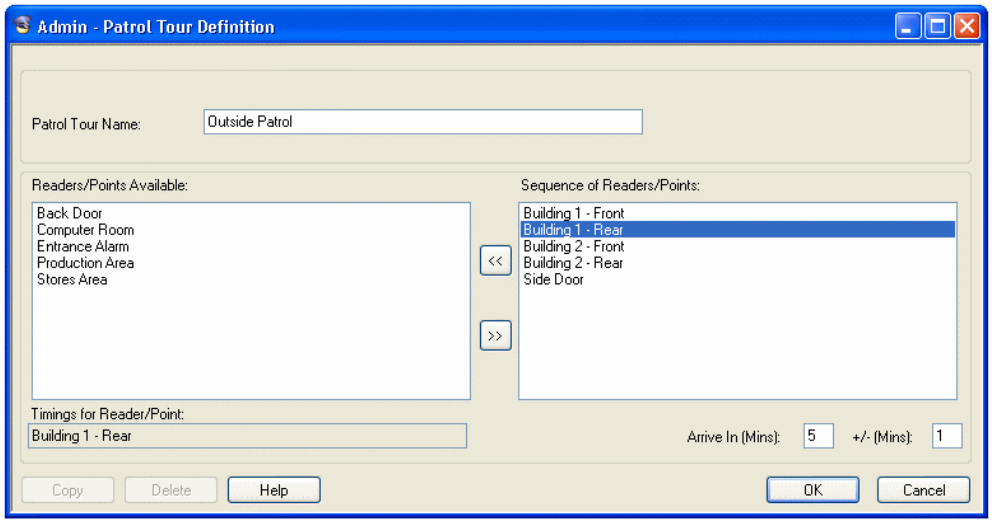


Par un changement du niveau de risque (dans la fenêtre Admin/Change Threat Level) on peut déterminer laquelle des cartes a accès à quelle zone et laquelle des commandes programmées et de déclenchement opèrent. Pour de plus amples informations, se référer aux manuels: *Threat Level Manager Installation* et *User Guide*.

La gestion des rondes des gardiens

Le manager des rondes des gardiens est un module optionnel pour configurer, rapporter et reproduire les rondes des gardiens. Le module comprend un jeu complet d'outils pour installer et gérer l'ensemble des rondes de contrôle au moyen du logiciel SMS. Il bénéficie de la possibilité de mettre en œuvre les lecteurs du contrôle d'accès comme points de contrôle des rondes, ce qui résulte des besoins pour un matériel non-spécialisé ou des appareils de collecte de données, de sorte qu'il soit d'une part prometteur pour la rentabilité et d'autre part facile à implanter en ce qui concerne l'introduction de la gestion des rondes.

Les rondes peuvent être prédéterminées d'une manière à spécifier la succession des points de contrôle à visiter et le temps admis pour le déplacement des gardiens entre ces points de contrôle.



La progression d'une ronde peut être surveillée, et les rondes précédentes se reproduisent dans des rapports. La capacité d'avertir immédiatement les opérateurs de SMS de toute infraction aux règles est un avantage particulier des applications de haute sécurité pour le système, une infraction comme des points de contrôle manqués ou leur desserte avec retard.

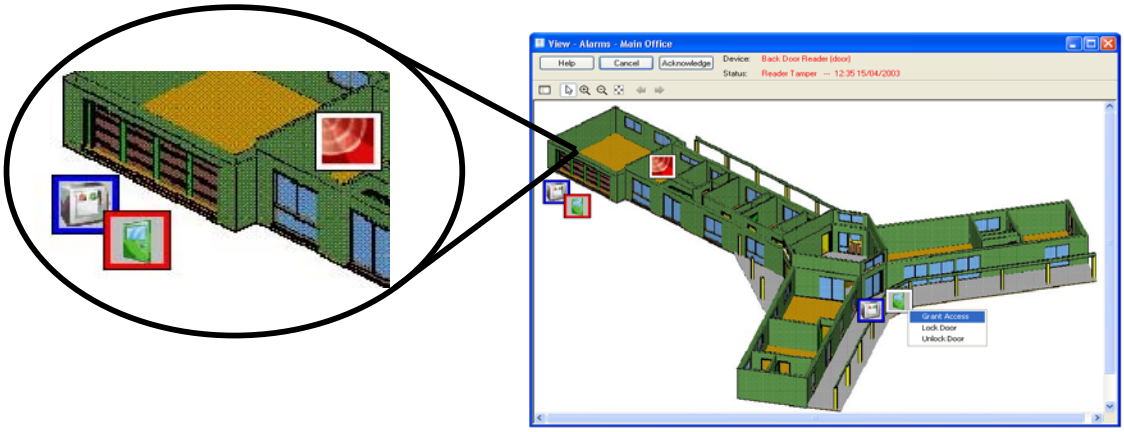
Le module fournit également une interface au logiciel connu GCS® TopGuard®. Le TopGuard facilite le contrôle d'un bon nombre de points sensibles, tels que fenêtres, extincteurs et clés, et pour le gardien il facilite le rapport de tout incident possible survenu pendant une ronde. La simple présentation d'un appareil de collecte de données comme le ProxiPen® à une petite balise rapporte la visite ou l'incident. L'interface transfère automatiquement tous les points de contrôle visités et tous les incidents rapportés au logiciel SMS aux fins d'un rapport centralisé et du traitement des alarmes.

Pour avoir plus d'informations, se référer aux *Guard Patrol Manager Installation et User Guide*.

La gestion des graphiques

L’ecran View/Graphics (Affichage/Graphiques) permet que des appareils comme les lecteurs, portes, caméras et capteurs CCTV sont faciles à surveiller par graphiques. Un graphique peut par exemple être un plan ou une cartographie du bâtiment.

Les graphiques peuvent afficher le statut d'alarme courrant de chaque dispositif contrôlé. Si le graphique est un plan, il est alors facile de situer une alarme et d'envoyer rapidement du personnel sur les lieux de l'incident, dirigé par une sécurité et efficacité améliorées de site.



Les graphiques installées dans l'écran Install/Graphics et configurées dans la fenêtre Configure/Graphics) peuvent contenir des liens à d’autres graphiques, ce qui permet à un opérateur de localiser une alarme ou un appareil avec une plus grande précision. Pour accélérer encore plus les temps de réaction, un graphique peut être installée pour afficher une alarme automatiquement dès qu’elle se produise.

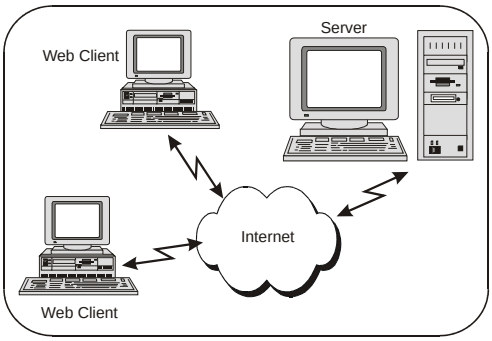
Les graphiques permettent aussi à un opérateur de contrôler les appareils. Un opérateur peut, par exemple, autoriser l'accès à une porte choisie, connecte à un interphone ou d’allumer la caméra CCTV d’un moniteur spécifié.

Les graphiques offrent une interface facile à utiliser pour la surveillance et le contrôle du système de gestion de sécurité. L’interface conçue d’une manière simple et intuitive permet au personnel de profiter des avantages d’usage des graphiques sans trop de notions préliminaires.

L’accès au Web

Le module optionnel Web Access permet à l’usager de surveiller, de contrôler et d’administrer le système de gestion de sécurité (SMS) en utilisant l’explorateur du Web de Microsoft via l'Internet ou l’Intranet de la société de l’usager.

En utilisant le module d’accès au Web, on a la possibilité de réaliser bon nombre de tâches, p.ex. installer le détenteur de carte, produire les badges, générer les rapports, surveiller les alarmes et enregistrer les éléments des visiteurs. Pour un Client Web il ne faut pas installer de drapeau ni de logiciel spécial, ce qui signifie un choix idéal pour les usagers qui nécessitent un accès temporaire au logiciel SMS depuis n’importe quel site.



L'interface utilisateur sur un Client Web est la même que pour un client standard du logiciel SMS. Ce fait permet aux usagers de profiter de tous les avantages à partir du logiciel convivial et d'économiser les dépenses générales requises pour apprendre une nouvelle interface utilisateur.

Les modes de lecteur

Les lecteurs sont bien sûr un élément principal du système de gestion de sécurité, et leur comportement doit être adapté aux exigences spécifiques sur le site.

Les lecteurs se règlent en plusieurs différents modes comme décrit ci-dessous.

Le mode de carte et PIN

En utilisant les commandes Card Only (carte seulement) et Card + PIN (carte + PIN) on peut commuter tout lecteur pourvu d'un clavier numérique entre les modes de carte seulement et carte et PIN. Pour un lecteur mis en mode de carte seulement il ne faut pas introduire un PIN pour avoir accès. En mode de carte et PIN il faut l'introduire, sauf si le détenteur de carte a des droits particuliers d'une carte générale (executive card), tels qu'ils sont installés dans la fenêtre Card Holder.

Il pourrait être bien de passer en mode de carte seulement lors des heures de pointe à l'aide d'une commande programmée.

Le mode du code utilisateur

Le mode du code utilisateur peut être utilisé aux lecteurs à clavier numérique. Un lecteur mis en mode du code utilisateur permet l'accès aux détenteurs de cartes sans présenter leurs cartes, mais en faisant le suivant:

1. appuyer sur le bouton #
2. entrer le numéro de carte (sans entrer les zéros dirigeants)
3. appuyer sur le bouton *

On n'a pas besoin de présenter la carte au lecteur (elle est pourtant acceptée comme à l'ordinaire).

On peut se servir du mode du code utilisateur en envoyant le code utilisateur seulement ou le code utilisateur + PIN au lecteur. Le mode du code utilisateur + PIN oblige les détenteurs de cartes à entrer aussi bien le PIN que le numéro de carte, tandis que le lecteur reste actif pour le mode du code utilisateur.

On peut désactiver le mode du code utilisateur en envoyant la commande User Code Disable au lecteur.

Le mode de commande de carte

Le mode de commande de carte permet au détenteur de carte pour lequel a été installée l'option dans la fenêtre Admin/Card Holder de générer des messages de commande de carte aux lecteurs à clavier numérique. Les messages peuvent servir avec des commandes de déclenchement à activer ou désactiver p.ex. des systèmes d'alarme d'intrusion, à allumer ou éteindre les éclairages ou à changer le PIN de carte ou les heures d'ouverture de porte.

Pour que le détenteur de carte puisse générer une commande de carte, il faut que le lecteur ait été réglé en ce mode, qu'il ait reçu à l'avance un ordre du mode de commande de carte. On peut désactiver le mode de commande de carte en envoyant l'instruction correspondante de Card Command Mode Off.

Le mode de carte-clé

Un détenteur de carte peut commuter un lecteur entre les états de „keycard-in" et de „keycard-out" (les droits d'accès devant le permettre) en présentant sa carte et en introduisant ensuite un PIN à quatre chiffres dans un ordre spécial, qui est de 3412 pour un PIN de 1234.

Lorsqu'un lecteur est en état de „keycard-out", il refuse l'accès à toutes les cartes, exceptées les cartes-clés, nonobstant les droits d'accès. Lorsqu'un lecteur est en état de „keycard-in", il est remis aux opérations ordinaires. Le mode carte-clé peut être utile, par exemple, dans des cas où une alarme anti-intrusion a besoin d'être armée et désarmée manuellement et uniquement par du personnel autorisé.

Le lecteur doit être paramétré pour les cartes clés dans l'écran Installation/Contrôle d'accès /Lecteur chaque personne qui a besoin de détenir une carte clé doit être pourvue du privilège sélectionné dans l'écran Administration/Détenteurs de cartes.

Vous pouvez armer ou désarmer le mode carte clé en envoyant la commande mode carte clé armé ou désarmé au lecteur. Vous pouvez mettre en mode de „keycard-in" ou „keycard-out" en utilisant la commande Keycard In ou Keycard Out.

Le mode du code client seulement

Ce mode permet l'accès à toute carte portant un code client valable, comme c'est configuré dans la fenêtre Facility/Customer Code du menu Configure. Dans ce mode tous les droits d'accès d'une carte sont annulés. Pour des informations plus détaillées se référer au programme d'aide *Online Help* sous View/Commands.

Le mode du code client seulement – le mode de non-mémorisation

Ce mode fonctionne de la même manière qu le mode Customer Code Only, sauf que les protocoles de chaque transaction ne sont pas sauvegardés.

Le mode Activer/Désactiver

Les commandes d'activer le lecteur et de désactiver le lecteur permettent de bloquer et de relancer le lecteur respectif. Un lecteur bloqué ne plus être utilisé par les gens.

Le mode d'empreinte digitale

Les lecteurs d'empreinte digitale peuvent être réglés de sorte qu'ils demandent juste une ou deux empreintes digitales en se servant des commandes du mode „Single Fingerprint" et du mode „Two Fingerprints". On peut annuler la condition de présenter une empreinte digitale en utilisant la commande de désactiver le mode „Fingerprint".

Le mode de contrainte (Duresss mode)

Un détenteur de carte peut aussi utiliser le PIN pour créer une alarme/un événement „contrainte“, en introduisant le PIN avec au début un zéro et en omettant le dernier chiffre. Une alarme/un événement „contrainte“ indiquent que le détenteur de carte a eu l’accès sous la contrainte. Le mode de contrainte ne s’applique qu’aux lecteurs pour lesquels on l’a installé dans la fenêtre Install/Access Control/Reader.

Le mode d’effacer suite à un PIN erroné

Si un détenteur de carte introduit un PIN incorrect, l’alarme/l’événement „Wrong PIN“ (mauvais PIN) sont signalés. Le système peut être équipé d’une manière à éviter qu’une carte passe, si le PIN est entré incorrectement à plusieurs reprises (nombre à spécifier). Le système ou nœud (selon le réglage préféré **Supprimer généralement en cas d’erreurs de PIN**) ne veut plus accepter la carte, ce qui génère l’alarme/l’événement „Deleted for PIN“ (supprimé à cause du PIN).

Le mode de bascule (Toggle mode)

Si un lecteur est actif en mode de bascule (dit toggle) dans la fenêtre Install/Access Control/Reader, chaque transaction du contrôle d’accès valable ou chaque demande valable de sortir (depuis un bouton de demande de sortie) a pour conséquence que la porte varie entre l’état constamment verrouillé et l’état constamment déverrouillé.

On pourrait prévoir ce mode p.ex. pour une entrée surveillée constamment dans la journée. Le matin le gardien se servirait de sa carte pour déverrouiller la porte en permanence, ensuite on surveillerait sur un écran de contrôle chaque personne entrant dans le bâtiment. Pour reverrouiller définitivement la porte, le gardien effectuerait – en sortant – une simple transaction du contrôle d’accès.

Le mode à deux cartes

Si un lecteur est mis en mode à deux cartes dans la fenêtre Install/Devices/Readers, il faut que deux transactions d’accès valables soient effectuées au lecteur à l’aide de deux différentes cartes, avant que l’accès ne soit possible. Les transactions sont à faire en l’espace d’un temps spécifié.

Ce mode s’applique dans des zones d’un bâtiment où la présence de plus d’une personne est d’importance.

Le mode d’inhibition du lecteur

Ce mode, d’habitude, il est utilisé pour ces lecteurs qui contrôlent les portes à tourniquet. Si un lecteur est réglé en mode d’inhibition dans la fenêtre Install/Access Control/Reader, il est en effet hors de service jusqu’à ce qu’un détenteur de carte ayant le droit d’accès ait passé une porte à tourniquet et cette dernière se verrouille à nouveau.

Les modes d’antipassback

Un lecteur peut être commuté en divers modes d’antipassback. Référez vous à *l'aide en ligne* pour de plus amples informations.

La sauvegarde et l’archivage des données

Une sauvegarde, qu’on peut faire en utilisant la fenêtre Tools/Backup, est une copie des fichiers du système, y compris des banques de données, des fichiers d’initialisation et d’encodage. La sauvegarde permet de reproduire les données p.ex. en cas d’un défaut de l’ordinateur.

Il est d'une importance incontournable de faire la sauvegarde régulièrement, le mieux tous les jours. Nous recommandons de sélectionner l'option de la sauvegarde préfixée à une heure exacte, p.ex. 4h00. C'est ainsi qu'on a assez de temps pour terminer les procédures prévues à minuit et pour certains sites extérieurs de télétransmettre leurs données du jour précédent. Le mieux serait d'éviter le temps autour de 2h00, sinon il y aurait une confusion lors du changement des heures d'été/hiver.

Une archive, qui peut être installée dans la fenêtre Tools/Archive, est une copie des bases de données historiques reçues de transactions, dans lesquelles sont cotenues les transactions de cartes, des alarmes, des événements, etc. Etablir des archives peut être nécessaire aux fins de rapports, dès que les données datent de plus longtemps qu'un nombre de jours spécifié et qu'elles sont effacées automatiquement, comme il est prévu par l'option **Purge Daily Logs After** (effacer les protocoles journaliers) dans la fenêtre Configure/Preferences .

Normalement l'intervalle entre les opérations d'archivage devrait être un peu inférieur à celui prévu par cette option **Purge Daily Logs After**. Exemple: Si l'option **Purge Daily Logs After** est fixée à un délai de 90 jours, on devrait procéder à l'archivage tous les 89 jours.

L'archivage dépend des exigences de chaque utilisateur, il n'est donc peut-être pas nécessaire; les données datant d'avant un temps à spécifier pouvant être sans intérêt. Il est à noter que dans le cas d'un recours à une archive pour reproduire un rapport, il faut réinsérer l'ensemble de l'archive dans la banque de données de transaction.

Installations pour multi-sociétés

Un des atouts principaux du système de gestion de sécurité consiste dans sa capacité de pouvoir servir à deux ou plusieurs sociétés qui seraient probablement bien conseillées de mettre en valeur ce produit en l'installant dans des bâtiments abritant plus d'un résidant.

Les bénéfices d'un système unique

Mettre en œuvre un système de gestion de sécurité unique plutôt qu'un système individuel pour chaque société promet de multiples avantages. Non seulement les frais pour l'équipement initial seront probablement moins chers, mais les frais courants aussi résultant par la suite des dépenses pour la sûreté devraient se réduire.

Une des économies essentielles des frais se calcule vraisemblablement pour les sites plus importantes, où on peut compter sur l'emploi le plus efficace d'un personnel de sécurité, car – si c'est nécessaire – un seul gardien peut surveiller les alarmes du site entier. Ceci peut se faire sur une base permanente ou – en cas de besoin – le système peut être installé d'une manière à faire diriger les alarmes vers un poste de surveillance central seulement la nuit, les jours fériés ou les week-ends, etc.

Dans des sites plus petits les sociétés ont la possibilité d'acheminer de cette manière les alarmes vers un point central et de partager les frais pour l'emploi d'un gardien, ce qui pourrait augmenter la sûreté de l'établissement.

Outre l'économie des frais un système unique met à profit d'importants avantages quant à la flexibilité. Si p.ex. un locataire a négocié l'utilisation d'autres parties du bâtiment, il n'y faut pas de câblage nouveau ni d'autres grands travaux, juste quelques petits réglages seront nécessairement à effectuer sur le PC. Ce degré de flexibilité vaut évidemment être pris en considération pour de nouveaux bâtiments, pour lesquels les conditions de bail ne sont peut-être pas encore définitivement conclues.

Groupes de sociétés – protéger les informations privées

Dans une installation à multi-sociétés, toutes leurs informations privées peuvent être protégées comme secrètes vis-à-vis des autres sociétés, un seul usager ayant le droit exclusif à l'accès de gestion de l'ensemble du système.

Pour protéger les informations privées, sont déterminées les autorisations de l'utilisateur (telles qu'elles sont installées dans la fenêtre Configure/User/Profiles) pour ces sociétés auxquelles il peut avoir accès. En allant dans les options du menu Admin, il peut installer, lire et éditer les informations des seules sociétés auxquelles il a l'autorisation d'accéder. On choisit la société spécifique pour le traitement en allant par l'option **Companies** du menu View.

En travaillant sur les informations d'une société, on peut normalement pas avoir un aperçu des informations installées pour d'autres sociétés. Il n'y a qu'une exception à cette règle, c'est lorsque l'option **Card Holders by Company** est désélectionnée dans la fenêtre Configure/Preferences/System. Si c'est le cas, on n'a accès qu'à lecture seule aux onglets détails de carte, données personnelles et biométriques dans la fenêtre Card Holder concernant chaque détenteur de carte de toutes les sociétés. On a également la possibilité d'ajouter et d'enlever les droits d'accès normaux en utilisant des lecteurs, groupes et codes de temps appartenant à la société choisie en ce moment. Ceci peut être utile, lorsque des lecteurs doivent servir aux employés de différentes sociétés.

Les options du menu View, exception faite de View/Alarms et de View/Activity, concernent également la seule société choisie en ce moment, lorsqu'on a sélectionné **View Menu by Company** dans la fenêtre Configure/ Preferences/System. S'il y a l'état désélectionné (implicite), les options concernent toutes les sociétés auxquelles on a le droit d'accéder.

Partager les appareils pour les droits d'accès

Chaque appareil tel que lecteur, point de surveillance et sortie auxiliaire est affecté à une société spécifique, ce qui assure à cette société d'avoir le contrôle exclusif de l'utilisation de leurs appareils.

Dans des situations pourtant, lorsqu'un lecteur doit être partagé par plus d'une société (p.ex. à l'entrée d'un bâtiment), la société 'propriétaire' peut ajouter le lecteur à un groupe de lecteurs partagé, de sorte que d'autres sociétés aient la possibilité d'intégrer le lecteur dans leurs droits d'accès.

Il en est de même pour les étages: Les espaces d'ascenseur devant être partagés peuvent s'ajouter aux groupes d'étage partagés.

Une procédure alternative: Utiliser l'option **Card Holders by Company**, voir plus haut.

Le routage des alarmes

On a toute la liberté d'acheminer les alarmes de chaque société vers un ou plusieurs PC-clients. Cette possibilité s'ajoute à celle de transférer les alarmes à différents ordinateurs du réseau en fonction de l'heure du jour, du jour de la semaine, voire même des jours fériés.

Un modem peut être mis en œuvre pour faire suivre automatiquement les alarmes à une installation complètement indépendante du système de gestion de sécurité. Ceci permet d'acheminer automatiquement les alarmes générées p.ex. sur un site laissé sans personne la nuit vers un site central gardé.

Les alarmes peuvent également être dirigées à une adresse de courrier électronique ou un messager de poche, à condition que l'option Email Alarms soit installée.

Index

A

Accès au Web....9-11
Alarmes
- acquitter....7-4
- comment elles sont utilisées....1-3
- comment les nouvelles alarmes sont signalées....7-1
- commentaires....7-5
- couleur....7-3
- démarches à faire....7-2
- effacer....7-6
- e-mail....1-3
- état....9-8
- filtres....7-3
- instructions....7-5
- listage....8-1
- localiser sur des graphiques....7-4
- nombre de....7-1
- priorité....7-1
- réinitialiser....7-6
- routage....9-16
- signification de....1-3
- surveillance....7-1
- voir les détails....7-2

Antipassback....9-14
Approuver la personne autorisée....4-4
Archives....9-14
Ascenseurs....3-8, 9-16

B

Badge....*Cf.* ID badge
Badge ID
- choisir la conception....4-5
- encoder....4-7
- imprimer....4-6
- prendre la photo....4-4
- saisir la signature....4-4
- saisir les données biométriques....4-5

Barre d'outils....2-2

Biométrie 4-5
Boîte d'alarmes 7-1
Bouton de silence 7-1
Boutons d'ouverture de porte
but 1-8

C

Caméra IP 6-1
Carte
commandes 3-5, 9-12
détails 3-4
encodage 3-3, 4-6
état 3-6
numéro 3-3
options 3-5
perdue/volée 3-6
PIN ..... *Cf.* PIN
Carte générale 3-5
Cartes de commande 3-5
Cartes inutilisées 3-6
Cas d'urgence 8-8
CCTV 1-11, 7-6
CCTV Caméras de surveillance 6-7
Changement des heures été/hiver 3-13
Client 1-8
clients Web 1-9
Code client 3-5
Code de service 3-5
Codes d'accès 3-8
Codes de temps
but 3-8
utilisés en commandes 9-5
Commandes
conditionnelles 9-6
installer 9-3
manuelles 9-3
programmées 9-4
Commandes prédéfinies 9-4
Communications
à distance 1-10
avec le nœud 1-10
Contrôle d'accès
signification 1-2
Contrôle jours fériés, dialogue 3-12
Coordonnées personnelles 3-13, 5-2
Copier 2-3
Cryptage 1-10

D

Demande de connexion 2-1
Détenteur de carte
conception du badge 4-5

coordonnées personnelles 3-13
créer 3-2
date active 3-4
détails 3-4
droits d'accès 3-7
fenêtre 3-1
imprimer un badge 4-4
localiser 3-15
nom 3-3
prendre la photo 4-4
recherche 3-14
rechercher 3-1
saisir la géométrie de la main ou l'empreinte digitale 4-5
saisir la signature 4-4
Commands 6-8
Digital video 1-11
commands 6-8
Droits d'accès
créer 3-7, 5-3
rapports 8-5
signification de 1-3

E

Edge-of-Network Video Server 1-11
Effacer 2-3
Effacer des alarmes 7-6
E-mail alarmes 1-3
Empreinte digitale 4-5
Encodage des cartes 4-7
Encoder Cartes 3-3
Encoder les cartes 4-6
Enregistreur numérique DVR (Digital Video Recorder) 6-1
Enterprise Edition 1-13
Entreprise
sociétés multiples 9-15
Entrer en connexion 7-1
ENVS 1-11
Etages
compris dans les droits d'accès 3-8
groupes de 3-8
partagés 9-16
Etat d'appareils 9-8
Evénements
comment ils sont utilisés 1-3
listage 8-1
signification de 1-3

F

Fall-back modem 1-10
Fenêtre
privilèges d'accès 9-1
Fenêtre alarmes 7-2

Fenêtre de sélection 2-3
Fenêtre Définition 2-3

G

Gestion centrale de cartes 1-14
Gestion de sécurité
- but 1-2
- composants de 1-7
- démarches pour installer le système 2-4
- fonctions optionnelles 1-5
- fonctions standard 1-5
- logiciel de départ 2-1
- types de produit 1-13

Global clients 1-13
Global Edition 1-13
Graphics 6-9, 9-10
Graphique 7-4
Groupes de sociétés 9-15

H

Handicapés 3-5
Heures 3-9

I

ID badge
- produire 4-1

Iinterface utilisateur 2-2
Import 4-5
Import Pad 4-5
Imprimante
- but 1-10

Imprimer les badges 4-6
Intégration vidéo numérique 6-1

J

Jours fériés 3-11

L

LAN 1-10
Lecteurs
- activer/désactiver 9-13
- but 1-7
- changer le mode d'opération 9-11
- compris dans les droits d'accès 3-8
- état 9-8
- groupes de 3-8
- mode d'empreinte digitale 9-13
- partagés 9-16
- verrouillage pour tourniquets 9-14

Lecteurs d'empreinte digitale 4-5
Listage d'accès 8-5
Lite Edition 1-13

Live 4-5
Localisateur 3-15
Locator 8-4
Log
sauvegarde et archivage 9-14
Logiciel de sauvegarde sur serveur vidéo 6-6
Logiciel du serveur de sauvegarde vidéo 6-1

M

M2000/M2100 ..... *Cf.* Nœuds
Mode à deux cartes 9-14
Mode d'empreinte digitale 9-13
Mode d'inhibition du lecteur 9-14
Mode d'utilisateur 9-12
Mode de bascule 9-13
Mode de carte et PIN 9-11
Mode de carte seulement 9-11
Mode de carte-clé 9-12
Mode de code client 9-13
Mode de commande de carte 3-5, 9-12
Mode de contrainte 3-5, 9-13
Modem
but 1-10
Mot de passe 2-1
multiNODE-2 ..... *Cf.* Nœuds

N

Niveaux de risque 9-8
Nodes
purpose of 1-10
Nœuds
communications 1-10
Nœuds
à distance 1-10
Nouveau 2-3

O

Options
permis de les utiliser 9-2

P

Password 9-1
PC
client 1-8
serveur 1-8
Photo 4-4
PIN
demande de mettre en/hors service 9-11
entrée incorrecte 9-13
entrer 9-11, 9-12
signaler une contrainte 3-5, 9-13
spécifier 3-5

Points de surveillance
but ... 1-11
état ... 9-8
groupes de ... 9-3
Porte
comprise dans les droits d'accès ... 3-8
moniteur ... 1-8
signification de ... 1-2
temps ... 3-5
verrous ... 1-8
Préférences ... 3-13, 9-14
Priorité de l'alarme ... 7-1
Professional Edition ... 1-13
Profiles ... 9-1

R

Rapport de présence
configurer ... 8-9
surveiller ... 8-10
usage ... 8-8
Rapport de présence en cas d'incendie ... 8-8
Rapport roll-call ... 8-8
Rapports
accès ... 8-5
activité ... 8-1
historique ... 8-2
présence ... 8-8
produire ... 8-1
roll-call ... 8-8
visiteur ... 5-3
Rapports d'événements ... 8-2
Rechercher ... 2-3
Reports
locator ... 8-4
Réseau ... 1-8
Rondes ... 9-9
Rondes des gardiens ... 9-9

S

Sauvegarde ... 9-14
Security management
window ... 2-2
Serveur ... 1-8
Société ... 9-16
Sorties auxiliaires
but ... 1-11
état ... 9-8
groupes de ... 9-3
Surveillance des alarmes ... 7-1
Système ENVS (Edge-of-Network Video Server) ... 6-1

T

Temps
accès 3-8, 3-9
Temps d'accès 3-9
Temps de porte étendus 3-5
Terminer la session 2-1
Tourniquets 9-14

U

Unité de géométrie de la main 4-5
Unité du connecteur 6-7
Utilisateurs
installer 9-1

V

Video verification 1-11
Visiteur
gestion 5-1
rapports 5-3